PIRNet: Privacy-Preserving Image Restoration Network via Wavelet Lifting

Xin Deng[1], Chao Gao[1], Mai Xu*[2]

[1]School of Cyber Science and Technology, Beihang University, Beijing, China
[2]School of Electronic and Information Engineering, Beihang University, Beijing, China
{cindydeng, EsthetGao, MaiXu}@buaa.edu.cn

Abstract

The cloud-based multimedia service becomes increasingly popular in the last decade, however, it poses a serious threat to the client's privacy. To address this issue, many methods utilized image encryption as a defense mechanism. However, the encrypted images look quite different from the natural images, making them vulnerable to attackers. In this paper, we propose a novel method namely PIRNet, which operates privacy-preserving image restoration in the steganographic domain. Compared to existing methods, our method offers significant advantages in terms of invisibility and security. Specifically, we first propose a wavelet Lifting-based Invertible Hiding (LIH) network to conceal the secret image into the stego image. Then, a Lifting-based Secure Restoration (LSR) network is utilized to perform image restoration in the steganographic domain. Since the secret image remains hidden throughout the whole image restoration process, the privacy of clients can be largely ensured. In addition, since the stego image looks visually the same as the cover image, the attackers can hardly discover it, which significantly improves the security. The experimental results on different datasets show the superiority of our PIRNet over the existing methods on various privacy-preserving image restoration tasks, including image denoising, deblurring and super-resolution.

1. Introduction

Recently, the cloud-based multimedia services have developed rapidly with the fast growing cloud computing technology. The Software-as-a-Service (SaaS) [5] such as Amazon Web Service (AWS) [1] and Google Cloud Platform (GCP) [2] provides strong computing resource to the clients, which allows them to perform efficient image processing online. However, image processing in the cloud poses a serious threat to the client's privacy. A hacker or a malicious service provider can easily access the clients' private photos, and discover their personal identity, social connections, and visited places for unauthorized uses.

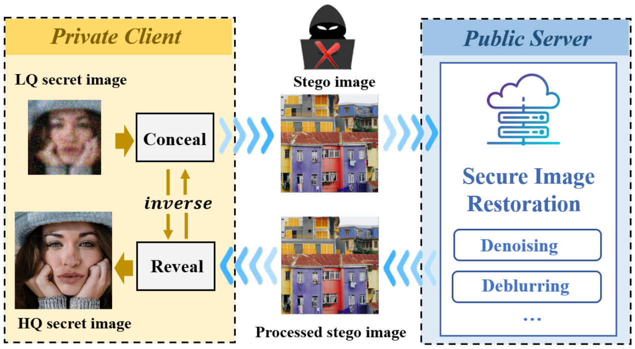

Figure 1. An illustration of the working process of the proposed method for privacy-preserving image restoration over cloud. The low-quality (LQ) secret image is first concealed into a stego image. Then, the secure image restoration is operated on the stego image to preserve privacy. Finally, the high-quality (HQ) secret image can be revealed from the processed stego image.

To tackle the security and privacy issue, many researchers have dived into the area of privacy-preserving image processing [17][34][28]. In these methods, image encryption is regarded as an important line of defense for privacy protection. They first utilized the homomorphic encryption [23] method to encrypt images. Then, the image processing is operated in the encrypted domain without decrypting the source image to achieve privacy protection. However, these encryption based methods have a big disadvantage, i.e., the encrypted images look quite different from the original images, making them more vulnerable to the attackers. Additionally, they rely on complex homomorphic crypto-system for encryption, which can be computationally heavy for real-time applications.

Different from the existing methods, we propose a novel method to operate privacy-preserving image restoration in the steganographic domain, which has a significant advan-

*Corresponding author

tage in terms of invisibility and security. As shown in Fig. 1, the steganographic technique allows the secret image to be concealed within the cover image, resulting in a stego image that looks quite similar to the cover one. That makes it quite difficult for attackers to detect the secret image. In addition, all restoration operations are performed on the stego images. *The secret image will not be disclosed both in image transmission and cloud server*, which can significantly reduce the risk of privacy leakage and breach. In addition to the above benefits, our approach does not require the complex homomorphic cryptosystem, which saves on computational cost. The success of our method relies on our important finding, i.e., when the image concealing and revealing processes are invertible, the quality change of the stego image can sensitively and stably affect the quality of the recovered secret image. The main contributions of this paper are summarized as follows:

- We propose a wavelet lifting based privacy-preserving image restoration network, namely PIRNet, to achieve confidential image restoration in steganographic domain without revealing the source image.
- We reveal an important finding about the correlation between the quality change of stego image and the restored secret image, which lays a great foundation for our network design for confidential image restoration.

2. Related Work

2.1. Privacy-Preserving Image Processing

In the recent decade, with the increasingly serious privacy disclosure in the cloud environment, many approaches have been proposed for privacy-preserving image processing. To protect privacy, most of these methods focus on the operation in encrypted domain [17, 34, 28]. Specifically, Lathey *et al.* [17] first attempted to perform image quality enhancement operations in the encrypted domain with Shamir's secret sharing technology (SSS) [25] as the encryption mechanism. Later, Ziad *et al.* [34] introduced a library which can perform several operations, such as edge sharpening and spatial filtering, on the encrypted image using the homomophic encryption. Based on the ramp secret sharing scheme[26], Tanwar *et al.* [28] proposed a method for image inpainting in the encrypted domain over the cloud. However, these methods rely upon sophisticated public-key homomophic cryptosystems, which are computationally heavy. In addition, since the encrypted images are visually different from the original ones, they can easily attract the attention from the attackers. Different from the above methods in the encrypted domain, our proposed PIRNet is performed in the steganographic domain which has a remarkable invisibility advantage. Since the stego image with secret information inside looks quite similar to the original cover image, it is difficult for the attacker to detect the secret image. Moreover, it can significantly save the computing costs since the complex homomophic cryptosystem is not needed. To the best of our knowledge, we are the first to explore privacy-preserving image restoration in steganographic domain.

2.2. Wavelet Lifting In Computer Vision Tasks

The lifting scheme was originally introduced in [27] as a technique to construct biorthogonal wavelets. Recently, the wavelet lifting scheme has been combined with deep networks, with well applications in various computer vision tasks [18, 12, 21]. Li *et al.* [18] first proposed to integrate CNN-based operators with the lifting scheme to construct the reversible blocks with good reversibility. Due to the perfect reconstruction property of wavelets, the reversible blocks are guaranteed to have strong stability and robustness. Based on these good characteristics, Huang *et al.* [12] proposed a wavelet-inspired invertible network to facilitate blind noise removal in images. Since the lifting scheme is information lossless, Ma *et al.* [21] combined wavelet lifting with deep compression network to perform lossless image compression. Inspired by wavelet lifting, the invertible neural networks (INNs) were proposed for memory saving and lossless transformation. With good reversibility, the INNs have made significant progress in many low-level computer vision tasks [20, 19, 10]. In this paper, our proposed method also benefits from the favorable characteristics of wavelet lifting, such as the multi-scale representations and reversibility, to achieve privacy-preserving image restoration in steganographic domain.

3. Method

3.1. Motivation

To achieve privacy-preserving image restoration, it is of significant importance to firstly find the suitable steganographic manipulated domain. Typically, the steganographic domain should meet the following requirements: the manipulation in the steganographic domain should be able to sensitively affect the results in the target restoration domain, and the influence should be stable and consistent. Regarding this issue, we have an important finding that the stego images generated by invertible image hiding network can meet the above requirements and act as a good steganographic domain. *The quality change of the stego image can sensitively affect the quality of the recovered secret image with good consistency.* Thus, by manipulating on the stego image, we can achieve the restoration of the secret image with good privacy protection. This interesting finding lays as a great foundation for our network design.

Analysis: In order to explore how changes in the stego image influence the recovered secret image, we design the following two experiments. The experiments are carried out on DIV2K [3] testing dataset with 100 images at resolution 1024×1024, and we randomly split it into 50 secret and 50 cover images. The Gaussian noise with standard deviation as 25 was added to the secret images. Then, the invertible image hiding network HiNet [14] was adopted to generate the stego images by hiding the noisy secret images into cover images. As expected, the stego images are also with noise.

In the first experiment, we apply three different image denoising networks including DnCNN[31], CBDNet[11] and RIDNet[4] to remove the noise in the stego images. The Peak Signal-to-Noise Ratio (PSNR) and Structural Similarity Index (SSIM) [29] are used to measure the quality of the stego image and recovered secret image. As shown in Fig. 2 (a) and (b), the higher quality of stego images leads to higher quality of the recovered secret image. Specifically, when the quality of stego image is improved from 28.18 dB to 28.56 dB by DnCNN, the corresponding recovered secret image is improved from 21.54 dB to 25.18 dB. This indicates that the manipulation of stego image can sensitively affect the quality of the recovered secret image. For more comprehensive demonstration, we carried out the second experiment, in which we degrade the quality of stego images by adding different levels of Gaussian noise, i.e., $\sigma = 5$, 10 and 15. The results are shown in Fig. 2 (c) and (d). As can be seen, when the quality of stego images decreases with higher noise level, the quality of recovered secret images gets worse correspondingly. These results demonstrate that the manipulation of stego image has consistent influences on the secret image.

From the above two experiments, we can conclude that the stego image is a good steganographic domain to perform privacy-preserving image restoration. Here, the invertible network plays an important role in closely relating steganographic domain and restoration domain. Thanks to the stable invertibility of invertible network, the steganographic domain can have a stable and consistent influence on the restoration domain, which brings significant benefits to privacy-preserving image restoration.

3.2. Framework

In this section, we propose a novel Privacy-preserving Image Restoration network, namely PIRNet, to achieve confidential image restoration in steganographic domain. Fig. 3 shows the overall framework of our PIRNet, which is composed of a Lifting-based Invertible Hiding (LIH) network and a Lifting-based Secure Restoration (LSR) network. For privacy protection, the LIH network is employed to conceal the secret image $\boldsymbol{x}_{secret}$ into a cover image $\boldsymbol{x}_{cover}$, to generate a stego image $\boldsymbol{x}_{stego}$. The $\boldsymbol{x}_{stego}$ is required to be indistinguishable from $\boldsymbol{x}_{cover}$ to improve the invisibility and security. Then, the stego image is sent to the LSR network for secure restoration. The LSR network is composed of K scales of wavelet lifting based secure restoration sub-nets, which can manipulate over the stego image without revealing the secret image. Finally, the stego image $\boldsymbol{x}'_{stego}$ after the LSR network is sent back to the LIH network to reveal the reconstructed high-quality (HQ) secret image $\boldsymbol{x}'_{secret}$.

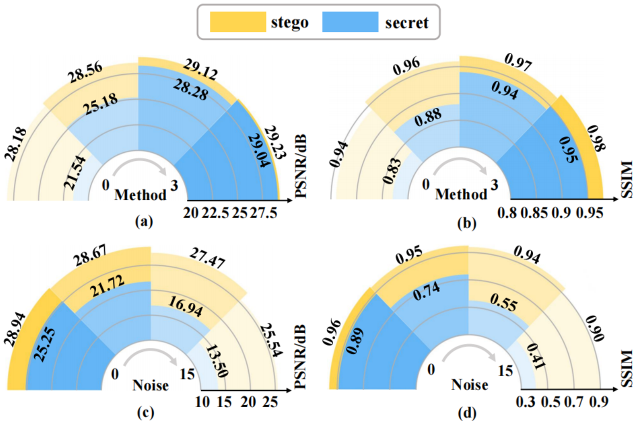

Figure 2. Correlation between the quality change of the stego image and the recovered secret image in terms of PSNR and SSIM. (a) and (b) represent the results with different denoising methods, in which method 0 represents the original results, and methods 1 to 3 represent the results with DnCNN, CBDNet and RIDNet, respectively. (c) and (d) represent the results by degrading the stego image with different Gaussian noise σ= 5, 10 and 15.

3.3. Lifting-based Invertible Hiding (LIH) Network

As demonstrated by our finding in Section 3.1, the invertible network is able to closely relate the steganographic domain and restoration domain, which is important for the privacy-preserving image restoration. Thus, we design a Lifting-based Invertible Hiding (LIH) network which can simultaneously hide three different types of degraded images, with noise, blur and low-resolution artifacts. The details of the LIH network are introduced as follows.

As can be seen in Fig. 3, the inputs to the LIH network are the degraded secret image $\boldsymbol{x}_{secret}$ and the cover image $\boldsymbol{x}_{cover}$. They are firstly decomposed into wavelet sub-bands $\boldsymbol{X}_{secret}$ and $\boldsymbol{X}_{cover}$ by Discrete Wavelet Transform (DWT). After that, the wavelet sub-bands are fed into several wavelet lifting (WL) blocks to generate the stego sub-bands $\boldsymbol{X}_{stego}$, together with the side information $\boldsymbol{R}$. The $\boldsymbol{R}$ contains the lost information in the forward concealing process, which is important to keep the invertibility of the LIH network. In the backward revealing process, since $\boldsymbol{R}$ is not available, we adopt an auxiliary variable $\boldsymbol{Z}$ which is assumed to have the same Gaussian distribution as $\boldsymbol{R}$. This is a common assumption as can be seen in other INN based networks [20, 10]. Then, the processed wavelet sub-bands $\boldsymbol{X}'_{stego}$ and a randomly sampled $\boldsymbol{Z}$ are sent back to the LIH network to reveal the reconstructed secret image.

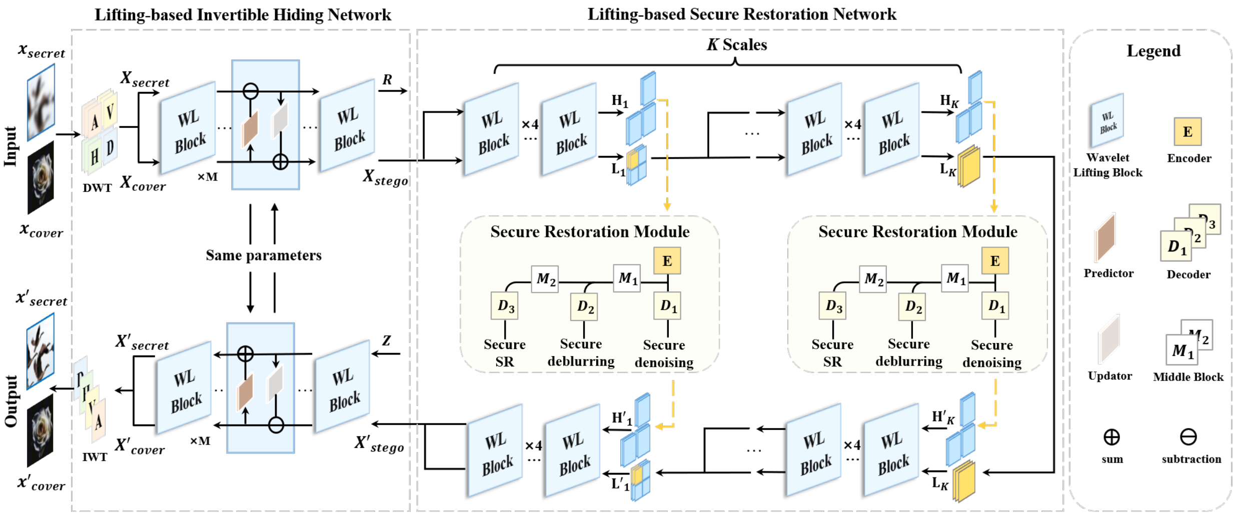

Figure 3. The architecture of the proposed Privacy-preserving Image Restoration network (PIRNet). The PIRNet consists of two parts: a Lifting-based Invertible Hiding (LIH) network and a Lifting-based Secure Restoration (LSR) network. The LSR network is composed of K scales of wavelet lifting based secure restoration sub-nets.

Wavelet Lifting (WL) Block. The wavelet lifting block is the basic unit of LIH network, which leverages a two-stream network structure to achieve the forward concealing and backward revealing processes. It should be noted that the forward and backward WL blocks share the same network parameters to guarantee the reversibility. There are in total M (M=24) WL blocks in the LIH network. For the i-th WL block in the forward concealing process, the inputs are $\boldsymbol{X}_{cover}^{i}$ and $\boldsymbol{X}_{secret}^{i}$, and the outputs $\boldsymbol{X}_{secret}^{i+1}$ and $\boldsymbol{X}_{cover}^{i+1}$ are formulated as follows,

$$\begin{aligned} \boldsymbol{X}_{secret}^{i+1} &= \boldsymbol{X}_{secret}^{i} - \boldsymbol{P}\left(\boldsymbol{X}_{cover}^{i}\right), \\ \boldsymbol{X}_{cover}^{i+1} &= \boldsymbol{X}_{cover}^{i} + \boldsymbol{U}\left(\boldsymbol{X}_{secret}^{i+1}\right), \end{aligned} \tag{1}$$

where $\boldsymbol{P}$ and $\boldsymbol{U}$ denotes the prediction and updating operations, respectively. Here, $\boldsymbol{P}$ and $\boldsymbol{U}$ can be any functions and their properties will not affect the reversibility. In this paper, we adopt the residual network for $\boldsymbol{P}$ and $\boldsymbol{U}$ due to its good trade-off between complexity and performance. For the i-th WL block in the backward revealing process, the inputs are $\boldsymbol{X}_{stego}^{i+1}$ and $\boldsymbol{Z}^{i+1}$, and the outputs $\boldsymbol{X}_{stego}^{i}$ and $\boldsymbol{Z}^{i}$ can be formulated as follows,

$$\begin{aligned} \boldsymbol{X}_{stego}^{i} &= \boldsymbol{X}_{stego}^{i+1} - \boldsymbol{U}\left(\boldsymbol{Z}^{i+1}\right), \\ \boldsymbol{Z}^{i} &= \boldsymbol{Z}^{i+1} + \boldsymbol{P}\left(\boldsymbol{X}_{stego}^{i}\right). \end{aligned} \tag{2}$$

Finally, after the first WL block, we can obtain the secret sub-bands $\boldsymbol{X}_{sr} = \boldsymbol{Z}^{1}$. They are then transformed back to the image through inverse wavelet transform.

Why Wavelet Lifting is Adopted for Hiding? As we know, there exist many deep image hiding networks [10, 6, 33]. In this paper, we propose a new wavelet lifting based invertible network for image hiding. There are three reasons behind our choice. 1) As demonstrated in [14], the wavelet domain is more appropriate for image hiding than pixel domain, especially the high-frequency sub-bands. The wavelet lifting scheme is originally designed for wavelet construction, which can naturally provide the wavelet manipulation domain. 2) The wavelet lifting scheme has the perfect reconstruction property [22], which can ensure the reversibility of hiding process. This is very important for the stability in confidential image restoration, as demonstrated in Section 3.1. 3) Our work focuses on the restoration of degraded images, and the key of it is to restore the high-frequent details. The wavelet lifting can naturally split the low and high-frequency details, which brings significant benefits to the image restoration task.

3.4. Lifting-based Secure Restoration (LSR)

The Lifting-based Secure Restoration (LSR) network is employed to perform different types of confidential image restorations including denoising, deblurring and super-resolution in the steganographic domain. Note that in LSR network, all restoration operations are performed on the stego images. The secret image will not be disclosed in LSR network, which can avoid the privacy disclosure. Next, we introduce the architecture of our LSR network in detail.

The LSR network is designed following the multi-scale property of wavelet lifting, which is composed of K scales of wavelet lifting based secure restoration sub-nets. Each sub-net consists of several WL blocks to update the low and high-frequency wavelet sub-bands, and a Secure Restoration Module (SRM) to perform restoration operations on the high-frequency sub-bands. As shown in Fig. 3, the input to the LSR network is $\boldsymbol{X}_{stego}$ generated by LIH. We first transform $\boldsymbol{X}_{stego}$ back to the image through inverse wavelet transform, and then use DWT to decompose the image into the new low-frequency and high-frequency wavelet sub-bands. For simplicity, we omit this transform process in Fig. 3. The low and high-frequency sub-bands are sent into the first-scale sub-net. After several WL blocks, we can obtain the updated low-frequency sub-band $\boldsymbol{L}_1$ and high-frequency sub-bands $\boldsymbol{H}_1$. The SRM module is then applied on $\boldsymbol{H}_1$ to generate the restored high-frequency sub-bands $\boldsymbol{H}_1'$ as follows,

$$\boldsymbol{H}_1' = f_{SRM}(\boldsymbol{H}_1). \tag{3}$$

For the low-frequency sub-band $\boldsymbol{L}_1$, we further split it by DWT and send the new sub-bands to the next scale sub-net, as shown in Fig. 3. Finally, after K scales, we can obtain $\boldsymbol{L}_K$ and $\boldsymbol{H}_K$. The $\boldsymbol{H}_K$ is processed by SRM to generate $\boldsymbol{H}_K'$, while the $\boldsymbol{L}_K$ is kept unchanged.

To keep consistency with the LIH network, the LSR network also has two inverse processes. The WL blocks in the forward and backward processes share the same network parameters. The backward process starts from the K-th scale, with $\boldsymbol{H}_K'$ and $\boldsymbol{L}_K$ as inputs. At the end of the backward process, we can obtain the restored wavelet sub-bands $\boldsymbol{X}_{stego}'$ of the stego image, which are then sent to the LIH network to restore the HQ secret image.

Secure Restoration Module (SRM). To deal with different types of degradation, we propose to design SRM as a multi-task learning [7] framework, as shown in Fig. 4. Specifically, the SRM is composed of an encoder and several decoders for different restoration tasks. All restoration tasks share the same encoder, which leads to better generalization ability and can save computing resources. As for decoding, considering that different restoration tasks have different levels of restoration difficulty, we unitize a hierarchical decoding architecture which is associated with the task difficulty. As can be seen from Fig. 4, we have three different tasks including image denoising, deblurring and super-resolution (SR). The SR task is the most difficult task, followed by deblurring and denoising. Thus, we extend extra middle blocks on top of the shared encoder for SR and deblurring tasks, and then connect them to the task-specific decoders. Here, the design of decoders are the same for all tasks. The encoder and decoder both follow the U-Net structure [24] with short cut, which is an efficient network design for image restoration. The NAFBlock [8] is adopted as the basic brick to build the encoder, decoder and middle blocks for its simplicity and good performance.

Why SRM is Applied Only on High-frequency Sub-bands? We apply SRM only on the high-frequency sub-bands of stego images for the following two reasons. First, in the LIH network, most information of the secret image is hidden in the high-frequency sub-bands of the stego image. Since our aim is to restore the secret image, it is better to perform on the high-frequency sub-bands. Second, the image degradation process loses the high-frequency details, and applying SRM on the high-frequency sub-bands can help better recover the lost image details.

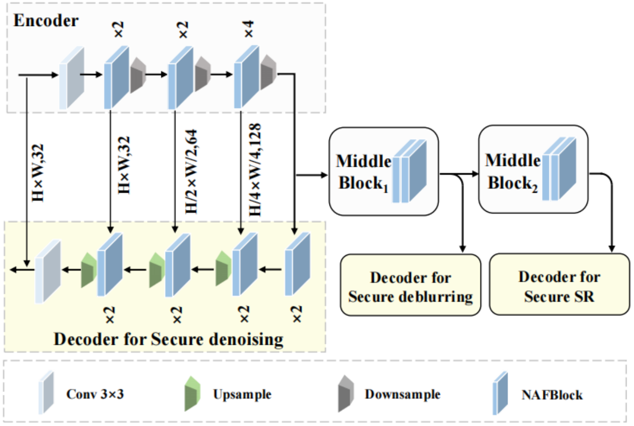

Figure 4. The architecture of Secure Restoration Module (SRM).

3.5. Training Strategy

In this paper, we use a multi-stage training procedure to train the PIRNet. In the first stage, we train the LIH network with the hiding loss. Then, we freeze the LIH to train the LSR network via the secure restoration loss. Finally, the whole network is fine-tuned in an end-to-end manner.

Hiding loss. The hiding loss is used to ensure the concealing and revealing performance of the LIH network, which is composed of three parts as follows,

$$L_{hid}(\Theta_H) = \lambda_{\mathcal{C}} L_{con} + \lambda_{\mathcal{R}} L_{rev} + \lambda_{\mathcal{F}} L_{freq}, \tag{4}$$

where $\lambda_{\mathcal{C}}$, $\lambda_{\mathcal{R}}$ and $\lambda_{\mathcal{F}}$ are the hyper-parameters for balancing different loss terms. The concealing loss L_{con} is used to make the stego image $\boldsymbol{x}_{stego}$ as similar as the cover image $\boldsymbol{x}_{cover}$, which is defined as follows,

$$L_{con} = \sum_{n=1}^{N} \ell_2 \left(\boldsymbol{x}_{stego}^{(n)}, \boldsymbol{x}_{cover}^{(n)} \right), \tag{5}$$

where N is the number of training samples. The revealing loss ensures that the revealed secret image $\boldsymbol{x}_{rs}$ is close to the original $\boldsymbol{x}_{secret}$. Thus, we define it as follows,

$$L_{rev} = \sum_{n=1}^{N} \mathbb{E}_{\boldsymbol{z} \sim p(\boldsymbol{z})} \ell_2 \left[(\boldsymbol{x}_{rs}^{(n)}, \boldsymbol{x}_{secret}^{(n)}) \right], \tag{6}$$

where $\boldsymbol{z}$ is an auxiliary variable randomly sampled from the distribution $p(\boldsymbol{z})$, as an important input to the backward revealing process of the LIH network. To improve the invisibility of stego images, we wish to hide the secret information into high-frequency sub-bands. That means the low frequency sub-band of stego image should be as similar as that of cover image. Thus, the low-frequency wavelet loss L_{freq} is defined as follows,

$$L_{freq} = \sum_{n=1}^{N} \ell_2 \left(\mathcal{H}(\boldsymbol{x}_{stego}^{(n)})_L, \mathcal{H}(\boldsymbol{x}_{cover}^{(n)})_L \right). \tag{7}$$

Here, $\mathcal{H}(\cdot)_L$ indicates the low-frequency wavelet sub-band.

Secure restoration loss. The secure restoration loss L_{sr} is used to train the LSR network. The goal is to make the restored HQ secret image $\boldsymbol{x}'_{secret}$ close to the ground-truth image $\boldsymbol{x}_{gt}$, while ensuring that the stego image after processing $\boldsymbol{x}'_{stego}$ and the cover image $\boldsymbol{x}_{cover}$ are as similar as possible. Thus, L_{sr} is composed of the following two parts,

$$L_{sr}(\Theta_R) = \lambda_{res} L_{res} + \lambda_{stego} L_{stego}. \tag{8}$$

Since the LSR network has a multi-task structure, the restoration loss L_{res} is hence described by,

$$L_{res} = \lambda_{\mathcal{N}} \ell_N + \lambda_{\mathcal{B}} \ell_B + \lambda_{\mathcal{S}} \ell_S, \tag{9}$$

where ℓ_N,ℓ_B and ℓ_S denote the loss of denoising, deblurring and super-resolution tasks, respectively. They can be uniformly defined as follows,

$$L_{\sharp} = \sum_{n=1}^{N} \ell_2 \left({\boldsymbol{x}'_{secret}}^{(n)}, \boldsymbol{x}_{gt}^{(n)} \right). \tag{10}$$

Here, $L_{\sharp}$ can be ℓ_N, ℓ_B or ℓ_S. The stego loss L_{stego} is used to ensure the similarity between $\boldsymbol{x}'_{stego}$ and $\boldsymbol{x}_{cover}$, which is defined as follows,

$$L_{stego} = \sum_{n=1}^{N} \ell_2 \left({\boldsymbol{x}'_{stego}}^{(n)}, \boldsymbol{x}_{cover}^{(n)} \right). \tag{11}$$

4. Experiment

4.1. Experiment Settings

Datasets and Settings. For network training and testing, we adopt the DIV2K dataset with 800 images for training and 100 images for testing. The image restoration tasks involve the typical image denoising, image deblurring and image super-resolution. During the training process, we use Gaussian noise with standard deviation from 0 and 55 to generate noisy secret images, and Gaussian blurring kernel with size ranging from 3 to 25 to generate blurred secret images. To produce low-resolution images, we apply bicubic downsampling to high-resolution images with 2× and 4× scaling factors. The number of scales in the LSR network is set as $K = 3$. In Eq. (4), the $\lambda_{\mathcal{C}}$, $\lambda_{\mathcal{R}}$ and $\lambda_{\mathcal{F}}$ are set to 2.0, 1.0 and 0.25, respectively. The λ_{res} and λ_{stego} in Eq. (9) are set to 3.0 and 1.0. The $\lambda_{\mathcal{N}}$, $\lambda_{\mathcal{B}}$ and $\lambda_{\mathcal{S}}$ in Eq. (10) are all set to 1.0. The network was trained with a NVIDIA 3090 GPU and optimized using the Adam method [15] with initial learning rate as 1×10^{-4}. The training batch size is 16, and the training epochs for the first and second stage are around 10K and 8K, respectively.

Comparison Methods. To the best of our knowledge, our work is the first privacy-preserving image restoration method in steganographic domain. Thus, for fair comparison, we create some new benchmarks by combining the state-of-the-art (SOTA) image hiding methods with SOTA image restoration methods to form a pipeline similar to our PIRNet. Specifically, for image hiding, we adopt HiDDeN [33], Balujia [6] and DeepMIH [10] methods. Here, the HiDDeN and Balujia are traditional CNN based hiding networks, while DeepMIH is based on invertible neural network. For image restoration, we adopt the SOTA NAFNet [8] and MIRNetv2 [30] for denoising, NAFNet [8] and XY-Deblur [13] for deblurring, and RLFN [16] and FMEN [9] for image super-resolution. We train these pipelines using the same dataset as ours, and the training process is consistent with our multi-stage training strategy.

Evaluation metrics. To evaluate the concealing and restoration performance of our method, we adopt three metrics to measure the quality of stego images and the restored secret images. The metrics include PSNR, SSIM[29] and LPIPS [32]. The larger value of PSNR and SSIM and smaller value of LPIPS indicate higher image quality.

4.2. Comparison against SOTA Methods

Quantitative results. Table 1 presents the denoising, deblurring and super-resolution results of our PIRNet and other comparison methods. As can be seen, our PIRNet achieves significantly better results than the comparison methods in terms of all three metrics for both $\boldsymbol{x}'_{stego}$/ $\boldsymbol{x}_{cover}$ and $\boldsymbol{x}'_{secret}$/$\boldsymbol{x}_{gt}$ image pairs. Here, $\boldsymbol{x}'_{stego}$ is the processed stego image after LSR network, and $\boldsymbol{x}'_{secret}$ is the restored high-quality secret image. Compared with the second best result, we improve the PSNR of $\boldsymbol{x}'_{secret}$/x_{gt} image pair by 2.11dB, 1.56dB and 0.79dB for denoising, deblurring and super-resolution tasks, respectively. For $\boldsymbol{x}'_{stego}$/ $\boldsymbol{x}_{cover}$ image pair, our PSNR is 0.37dB, 0.65dB and 2.96dB higher than the second best results for these three tasks, respectively. Such quality superiority is also indicated in the other metrics, which shows the effectiveness of our PIRNet.

Qualitative analysis. Fig. 5 visualizes the stego image processed by LSR network and restored HQ secret image of different methods. As can be seen, our restored secret images are very clean, with rich details and clear edges. In addition, the stego image of our method is nearly indistinguishable from the cover image, indicating the good confidentiality of our method. In contrast, the stego images of the comparison methods have obvious texture-copying artifacts and color distortion. Besides, their restored secret images still contain blurred edges and artifacts.

4.3. Ablation Study

Effectiveness of the multi-scale scheme in LSR network. As we mentioned before, the LSR network is designed following the multi-scale property of wavelet lifting, which is composed of K scales of restoration sub-nets. To explore the effectiveness of the multi-scale scheme, we set the scale number K to be 1, 2 and 3 to see how the restora-

Table 1. Comparison results in terms of PSNR and SSIM for denoising ($\sigma = 25$), deblurring (kernel size is 15), and super-resolution (4× upscaling factor). The best results are in bold and second bests are underlined.

Task	Method	x'_{stego}/ x_{cover} image pair			x'_{secret}/x_{gt} image pair		
		PSNR (dB)↑	SSIM↑	LPIPS↓	PSNR (dB)↑	SSIM↑	LPIPS↓
Denoise	HiDDeN[33]+MIRNetV2[30]	24.26	0.9226	0.311	25.95	0.8920	0.356
	HiDDeN[33]+NAFNet[8]	22.18	0.9206	0.321	25.22	0.8785	0.378
	Baluja[6]+MIRNetV2[30]	28.66	0.9708	0.212	23.17	0.8584	0.516
	Baluja[6]+NAFNet[8]	24.91	0.9424	0.318	25.51	0.8774	0.361
	DeepMIH[10]+MIRNetV2[30]	29.02	0.9542	0.260	27.10	0.9185	0.327
	DeepMIH[10]+NAFNet[8]	28.77	0.9631	0.225	26.40	0.9033	0.346
	Ours	**29.39**	**0.9775**	**0.185**	**29.21**	**0.9556**	**0.110**
Deblur	HiDDeN[33]+XYDeblur[13]	24.27	0.9423	0.275	25.72	0.9186	0.383
	HiDDeN[33]+NAFNet[8]	25.29	0.9356	0.233	21.67	0.8669	0.510
	Baluja[6]+XYDeblur[13]	28.06	0.9710	0.225	27.17	0.9467	0.258
	Baluja[6]+NAFNet[8]	28.81	0.9727	0.220	22.45	0.8278	0.549
	DeepMIH[10]+XYDeblur[13]	29.02	0.9845	0.178	25.76	0.9362	0.385
	DeepMIH[10]+NAFNet[8]	29.47	0.9844	0.159	25.63	0.9324	0.392
	Ours	**30.12**	**0.9851**	**0.150**	**28.73**	**0.9701**	**0.139**
Super-resolution	HiDDeN[33]+RLFN[16]	21.02	0.9254	0.338	22.28	0.8427	0.457
	HiDDeN[33]+FMEN[9]	20.39	0.9330	0.305	21.43	0.8351	0.507
	Baluja[6]+RLFN[16]	23.30	0.9634	0.285	22.64	0.8417	0.531
	Baluja[6]+FMEN[9]	23.91	0.9628	0.276	22.81	0.8417	0.457
	DeepMIH[10]+RLFN[16]	27.37	0.9747	0.220	23.72	0.8892	0.460
	DeepMIH[10]+FMEN[9]	26.78	0.9689	0.230	23.67	0.8872	0.452
	Ours	**30.33**	**0.9863**	**0.139**	**24.51**	**0.9017**	**0.261**

Table 2. Ablation study on the scale number of LSR network.

Task	Scales	x'_{secret}/x_{gt} image pair		
		PSNR (dB)↑	SSIM↑	LPIPS↓
Denoise	K=1	29.00	0.9534	0.117
	K=2	29.12	0.9547	0.112
	K=3	**29.21**	**0.9556**	**0.110**
Deblur	K=1	28.28	0.9665	0.158
	K=2	28.69	0.9670	0.141
	K=3	**28.73**	**0.9701**	**0.139**
Super-resolution	K=1	24.34	0.8985	0.270
	K=2	24.44	0.9007	0.265
	K=3	**24.51**	**0.9017**	**0.261**

Table 3. Ablation study on the reversibility of LIH network.

Task	Reversibiliy	x'_{secret}/x_{gt} image pair		
		PSNR (dB)↑	SSIM↑	LPIPS↓
Denoise	✗	27.96	0.9483	0.156
	✓	**29.21**	**0.9556**	**0.110**
Deblur	✗	27.35	0.9667	0.215
	✓	**28.73**	**0.9701**	**0.139**
Super-resolution	✗	22.73	0.8927	0.303
	✓	**24.51**	**0.9017**	**0.261**

tion performance changes with the scale number. The results are shown in Table 2. As can be seen, the PSNR value gradually increases with the number of scales, for all the three restoration tasks. Specifically, when K is increased from 1 to 3, the PSNR value increases by 0.21dB, 0.45dB and 0.17dB for denoising, deblurring and SR tasks, respectively. The possible reason is that multi-scale property of wavelets can capture and process more detailed information, which brings benefits to the restoration.

Effectiveness of the reversibility of LIH network. In the LIH network, we model the revealing as the inverse process of concealing. To verify the effectiveness of this reversibility, we trained another network in which the concealing and revealing processes are irreversible. The results are shown in Table 3. As can be seen, without the reversibility, the restoration performance significantly drops for all the three tasks. The reason is that the reversibility plays important roles to keep the stability between steganographic domain and restoration domain. Once the reversibility is broken, the relationship between the steganographic and restoration domains becomes volatile and inconsistent, which harms the restoration performance.

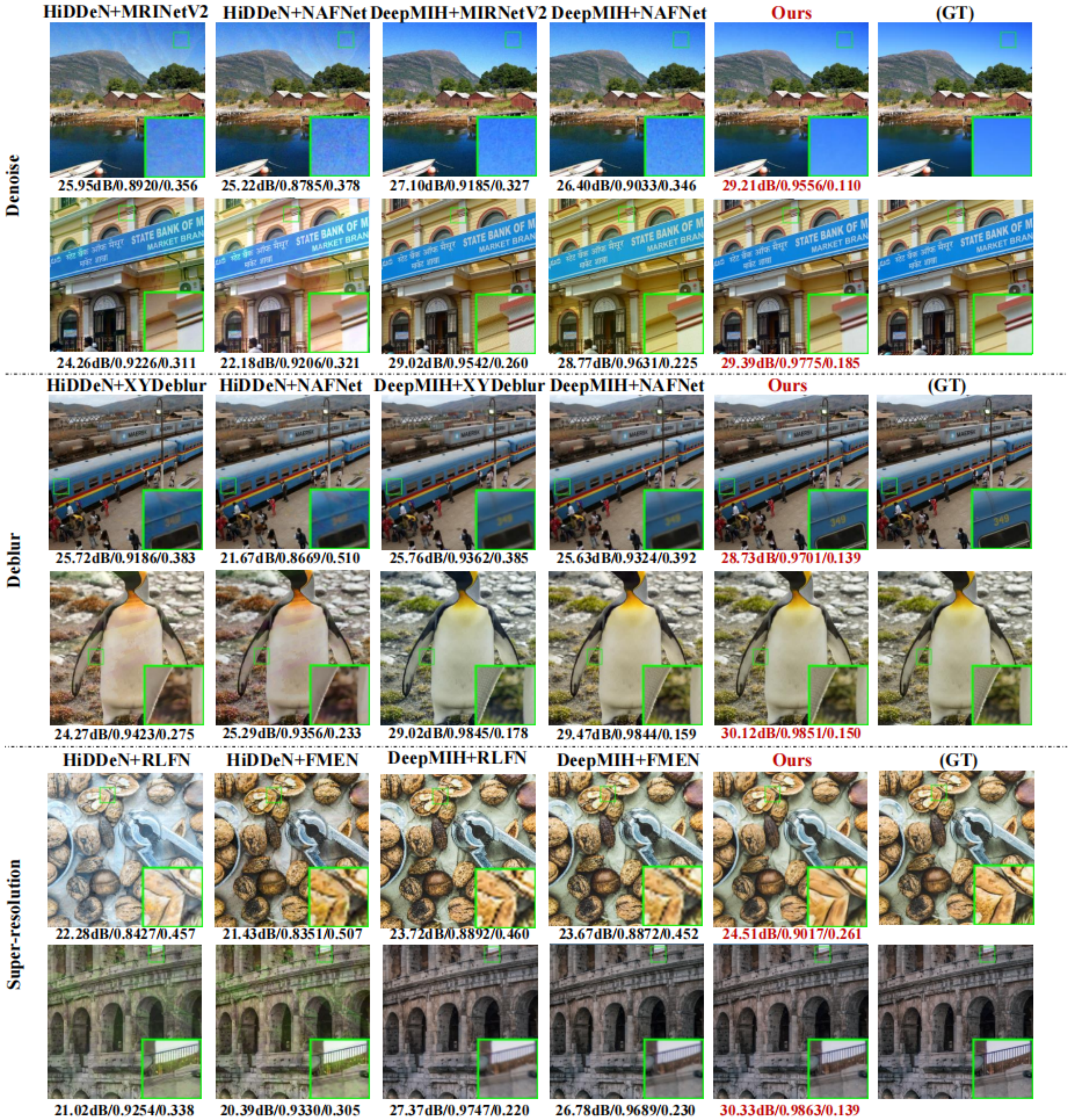

Figure 5. The visualizations of the recovered HQ secret image (first row of each task) and the stego image proccessed by LSR network (second row of each task) by different methods. The numbers in the brackets indicate the PSNR/SSIM/LPIPS values.

5. Conclusion

In this paper, we introduce a new approach for privacy-preserving image restoration in the steganographic domain, which provides significant benefits in terms of invisibility and security. The success of our method relies on our important finding, i.e., *the quality change of the stego image can sensitively and consistently affect the quality of the recovered secret image.* Thus, by manipulating in the steganographic domain, we can achieve privacy-preserving restoration of the secret image. Extensive experimental results show that our method can achieve good image restoration performance both quantitatively and qualitatively, while ensuring the security of the secret image.

Acknowledgments. This work is supported by National Natural Science Foundation of China under Grants 62001016, 62231002, 62250001, and Young Elite Scientists Sponsorship Program 2022QNRC001 by CAST.

References

[1] Amazon Web Services. https://aws.amazon.com/. Accessed: March 7, 2023. 1

[2] Google Cloud Platform. https://cloud.google.com/. Accessed: March 5, 2023. 1

[3] Eirikur Agustsson and Radu Timofte. Ntire 2017 Challenge on Single Image Super-resolution: Dataset and Study. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops*, pages 126–135, 2017. 3

[4] Saeed Anwar and Nick Barnes. Real Image Denoising With Feature Attention. In *2019 IEEE/CVF International Conference on Computer Vision (ICCV)*, pages 3155–3164, 2019. 3

[5] Michael Armbrust, Armando Fox, Rean Griffith, Anthony D Joseph, Randy Katz, Andrew Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica, and et al. A View of Cloud Computing. *Communications of the ACM*, 53(4):50–58, 2010. 1

[6] Shumeet Baluja. Hiding Images in Plain Sight: Deep Steganography. In I. Guyon, U. Von Luxburg, S. Bengio, H. Wallach, R. Fergus, S. Vishwanathan, and R. Garnett, editors, *Advances in Neural Information Processing Systems*, volume 30. Curran Associates, Inc., 2017. 4, 6, 7

[7] Rich Caruana. Multitask Learning: A Knowledge-Based Source of Inductive Bias. In *Proceedings of the Tenth International Conference on International Conference on Machine Learning*, ICML'93, page 41–48, San Francisco, CA, USA, 1993. Morgan Kaufmann Publishers Inc. 5

[8] Liangyu Chen, Xiaojie Chu, Xiangyu Zhang, and Jian Sun. Simple Baselines for Image Restoration. In Shai Avidan, Gabriel Brostow, Moustapha Cissé, Giovanni Maria Farinella, and Tal Hassner, editors, *Computer Vision – ECCV 2022*, pages 17–33, Cham, 2022. Springer Nature Switzerland. 5, 6, 7

[9] Zongcai Du, Ding Liu, Jie Liu, Jie Tang, Gangshan Wu, and Lean Fu. Fast and Memory-Efficient Network Towards Efficient Image Super-Resolution. In *2022 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*, pages 852–861, 2022. 6, 7

[10] Zhenyu Guan, Junpeng Jing, Xin Deng, Mai Xu, Lai Jiang, Zhou Zhang, and Yipeng Li. DeepMIH: Deep Invertible Network for Multiple Image Hiding. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 45(1):372–390, 2022. 2, 3, 4, 6, 7

[11] Shi Guo, Zifei Yan, Kai Zhang, Wangmeng Zuo, and Lei Zhang. Toward Convolutional Blind Denoising of Real Photographs. In *2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, pages 1712–1722, 2019. 3

[12] Jun-Jie Huang and Pier Luigi Dragotti. WINNet: Wavelet-Inspired Invertible Network for Image Denoising. *IEEE Transactions on Image Processing*, 31:4377–4392, 2022. 2

[13] Seo-Won Ji, Jeongmin Lee, Seung-Wook Kim, Jun-Pyo Hong, Seung-Jin Baek, Seung-Won Jung, and Sung-Jea Ko. XYDeblur: Divide and Conquer for Single Image Deblurring. In *2022 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, pages 17400–17409, 2022. 6, 7

[14] Junpeng Jing, Xin Deng, Mai Xu, Jianyi Wang, and Zhenyu Guan. HiNet: Deep Image Hiding by Invertible Network. In *2021 IEEE/CVF International Conference on Computer Vision (ICCV)*, pages 4713–4722, 2021. 3, 4

[15] Diederik P Kingma and Jimmy Ba. Adam: A Method for Stochastic Optimization. *arXiv preprint arXiv:1412.6980*, 2014. 6

[16] Fangyuan Kong, Mingxi Li, Songwei Liu, Ding Liu, Jingwen He, Yang Bai, Fangmin Chen, and Lean Fu. Residual Local Feature Network for Efficient Super-Resolution. In *2022 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*, pages 765–775, 2022. 6, 7

[17] Ankita Lathey and Pradeep K Atrey. Image Enhancement in Encrypted Domain over Cloud. *ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM)*, 11(3):1–24, 2015. 1, 2

[18] Shaohui Li, Wenrui Dai, Ziyang Zheng, Chenglin Li, Junni Zou, and Hongkai Xiong. Reversible Autoencoder: A CNN-Based Nonlinear Lifting Scheme for Image Reconstruction. *IEEE Transactions on Signal Processing*, 69:3117–3131, 2021. 2

[19] Shaohui Li, Ziyang Zheng, Wenrui Dai, Junni Zou, and Hongkai Xiong. REV-AE: A Learned Frame Set for Image Reconstruction. In *ICASSP 2020-2020 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pages 1823–1827. IEEE, 2020. 2

[20] Yang Liu, Zhenyue Qin, Saeed Anwar, Pan Ji, Dongwoo Kim, Sabrina Caldwell, and Tom Gedeon. Invertible Denoising Network: A Light Solution for Real Noise Removal. In *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition*, pages 13365–13374, 2021. 2, 3

[21] Haichuan Ma, Dong Liu, Ning Yan, Houqiang Li, and Feng Wu. End-to-end optimized versatile image compression with wavelet-like transform. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 44(3):1247–1263, 2020. 2

[22] S.G. Mallat. A Theory for Multiresolution Signal Decomposition: The Wavelet Representation. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 11(7):674–693, 1989. 4

[23] Ronald L. Rivest and Michael L. Dertouzos. ON DATA BANKS AND PRIVACY HOMOMORPHISMS. 1978. 1

[24] Olaf Ronneberger, Philipp Fischer, and Thomas Brox. U-Net: Convolutional Networks for Biomedical Image Segmentation. *Medical Image Computing and Computer-Assisted Intervention (MICCAI)*, 9351:234–241, 2015. 5

[25] Adi Shamir. How to Share a Secret. In *Communications of the ACM*, volume 22, pages 612–613. ACM, 1979. 2

[26] Xiaolei Sun, Dongdai Lin, and Qiong Huang. Ramp Secret Sharing Scheme with Authenticated Recovery. In *Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'05)*, pages 324–329. IEEE, 2005. 2

[27] Wim Sweldens. Lifting Scheme: A New Philosophy in Biorthogonal Wavelet Constructions. In *Wavelet applications in signal and image processing III*, volume 2569, pages 68–79. SPIE, 1995. 2

[28] Vishesh Kumar Tanwar, Balasubramanian Raman, Amitesh Singh Rajput, and Rama Bhargava. 2DInpaint: A Novel Privacy-preserving Scheme for Image Inpainting in An Encrypted Domain over the Cloud. *Signal Processing: Image Communication*, 88:115931, 2020. 1, 2

[29] Zhou Wang, Alan C Bovik, Hamid R Sheikh, and Eero P Simoncelli. Image Quality Assessment: from Error Visibility to Structural Similarity. *IEEE Transactions on Image Processing*, 13(4):600–612, 2004. 3, 6

[30] Syed Waqas Zamir, Aditya Arora, Salman Khan, Munawar Hayat, Fahad Shahbaz Khan, Ming-Hsuan Yang, and Ling Shao. Learning Enriched Features for Fast Image Restoration and Enhancement. *IEEE Transactions on Pattern Analysis and Machine Intelligence (TPAMI)*, 2022. 6, 7

[31] Kai Zhang, Wangmeng Zuo, Yunjin Chen, Deyu Meng, and Lei Zhang. Beyond a Gaussian Denoiser: Residual Learning of Deep CNN for Image Denoising. *IEEE Transactions on Image Processing*, 26(7):3142–3155, 2017. 3

[32] Richard Zhang, Phillip Isola, Alexei A Efros, Eli Shechtman, and Oliver Wang. The Unreasonable Effectiveness of Deep Features as a Perceptual Metric. In *CVPR*, 2018. 6

[33] Jiren Zhu, Russell Kaplan, Justin Johnson, and Li Fei-Fei. HiDDeN: Hiding Data with Deep Networks. In *Proceedings of the European conference on computer vision (ECCV)*, pages 657–672, 2018. 4, 6, 7

[34] M Tarek Ibn Ziad, Amr Alanwar, Moustafa Alzantot, and Mani Srivastava. Cryptoimg: Privacy Preserving Processing over Encrypted Images. In *2016 IEEE Conference on Communications and Network Security (CNS)*, pages 570–575. IEEE, 2016. 1, 2