PRNet: A Progressive Recovery Network for Revealing Perceptually Encrypted Images

Tao Xiang[1], Ying Yang[1], Shangwei Guo[1], Hangcheng Liu[1], Hantao Liu[2]

[1] Chongqing University, [2] Cardiff University

Contact: swguo@cqu.edu.cn

Problem Definition and Related Work

Perceptual Encryption:

- *Perceptual Encryption*: An efficient way of protecting the visual content of images by considering the characteristics of image data.
- *Cryptanalysis*: differential attacks, linear attacks and other statistical analysis methods.

Attack Goal: Reveal all the secret content from encrypted images without any prior knowledge about the encryption algorithm.

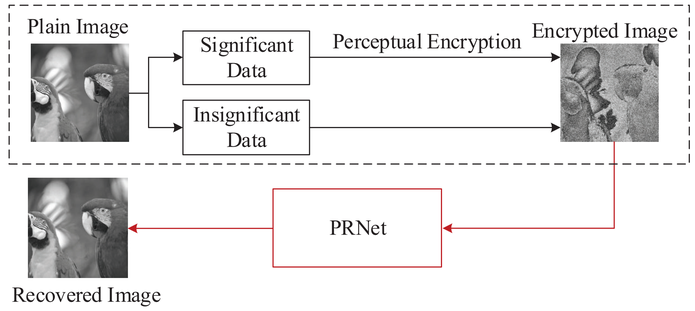
- *Encryption-Agnostic*: No knowledge about the encryption algorithm, such as every single detail of the encryption procedure and the distortion pattern of the encrypted images.
- *Efficient*: Attack perceptually encrypted images in an end-to-end manner.
- *Effective*: Recover secret content of high quality compared with existing traditionalcryptanalysis methods and state-of-the-arts CNN-based image restoration solutions.

Related Work:

- Traditional Cryptanalysis: Require strict prior knowledge of the encryption algorithm and involve heavy manual work.
  NOT encryption-agnostic and efficient
- CNN-Based Image Restoration: Focus on high/medium-quality images with fixed-pattern and normally-distributed distortions, while distortions caused by encryption are unevenly distributed and have no pattern to follow.
  NOT effective

Overall Attack Procedure:

- *Training*: Generate a perceptually encrypted image dataset and train our PRNet.
- *Attacking*: Recover the plain image of a given encrypted image using the trained PRNet.

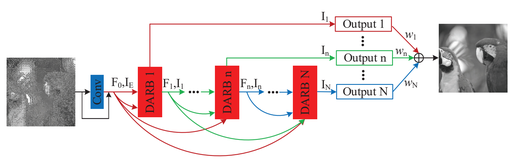


Proposed Method

Key Insights:

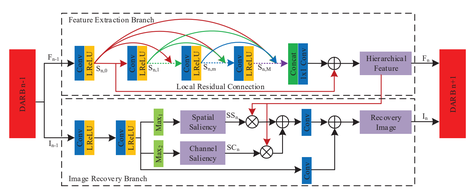
- Train an end-to-end model to memorize the relationships between encrypted images and plain images ***without*** any manual work or prior knowledge.
- Design dense attention recovery blocks to ***recover*** more detailed visual content about the plain image from the encrypted one and thus ***enhance*** the visual quality of the recovered images.

Progressive Recovery Network (PRNet):



- Our PRNet is stacked with several dense attention recovery blocks (DARBs) to progressively recover visual content from encrypted image.

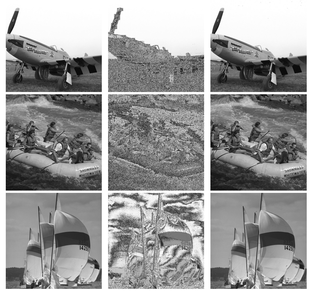
Dense Attention Recovery Block (DARB):



- Each DARB contains two branches: feature extraction branch and image recovery branch.

Attack Result

Attack Results by Our PRNet:



- Left column: Plain images; Middle column: Cipher images encrypted by MBSE, GLSE and RISE peceptual encryption algorithm, respectively; Right column: Recovered high-quality images using the proposed PRNet.
- Perceptual encryption leads to heavy corruptions on image visual content. PRNet can ***reconstruct*** the detailed visual content and ***remove*** the artifacts created by encryption. The recovered images are very close to the plain images.

Experiments & Results

Quantitative Results on Kodak24 Database:

Method	MBSE	GLSE	RISE
	PSNR / SSIM / LFBVS / IIBVSI	PSNR / SSIM / LFBVS / IIBVSI	PSNR / SSIM / LFBVS / IIBVSI
Encryption	13.93 / 0.375 / 0.650 / 0.412	15.02 / 0.189 / 0.563 / 0.451	11.26 / 0.133 / 0.482 / 0.323
SRCNN	21.28 / 0.622 / 0.824 / 0.519	19.35 / 0.567 / 0.792 / 0.555	30.91 / 0.839 / 0.896 / 0.848
FSRCNN	21.58 / 0.645 / 0.820 / 0.527	19.91 / 0.593 / 0.830 / 0.552	38.55 / 0.953 / 0.935 / 0.936
VDSR	22.94 / 0.738 / 0.859 / 0.653	27.32 / 0.901 / 0.944 / 0.922	46.80 / 0.994 / 0.963 / 0.964
LapSRN	23.48 / 0.769 / 0.878 / 0.694	27.09 / 0.937 / 0.943 / 0.917	41.78 / 0.939 / 0.947 / 0.941
MemNet	21.43 / 0.671 / 0.827 / 0.575	24.72 / 0.690 / 0.810 / 0.707	26.66 / 0.720 / 0.851 / 0.741
RDN	23.52 / 0.760 / 0.877 / 0.691	36.78 / 0.975 / 0.961 / 0.948	39.99 / 0.928 / 0.943 / 0.906
PRNet (ours)	25.27 / 0.817 / 0.905 / 0.751	36.99 / 0.987 / 0.963 / 0.949	49.50 / 0.990 / 0.975 / 0.978

- Quantitative experimental results of the proposed PRNet and compared state-of-the-art CNN-based image restoration methods on three different perceptual encryption algorithms, including MBSE, GLSE and RISE. Red and Blue colors indicate the best and second best performance, respectively.

Qualitive Results on MBSE Algorithm:

- The attacking results of our PRNet and compared CNN-based image restoration methods on MBSE algorithm.