Joint compressive autoencoders for full-image-to-image hiding

Xiyao Liu[1], Ziping Ma[1], Xingbei Guo[1], Jialu Hou[1], Lei Wang[1], Jian Zhang[1], Gerald Schaefer[2], Hui Fang[2]
[1]School of Computer Science and Engineering, Central South University [2]Department of Computer Science Loughborough University

Background

- Classical Image hiding methods can't embed a image into a same-sized cover image.
- Deep learning based methods are exploited to further improve the hidden capacity and can embed images into a same-sized image.
- Exsiting deep learning based methods minimises both reconstruction errors of cover and secret images, meaning **neither of these errors can be minimised**.

Motivation & Key Contributions

- **Motivation:** (i) Increase the hidden capacity. (ii) Solve the important trade-off problem in DL-based methods . (iii) Ensure the security.
- **Key Contributions:** (i) Firstly and fundamentally avoids the trade-off problem for effective full-image-to-image hiding. (ii) Ensures high recovery quality of hidden images. (iii) A logistic-logistic chaotic mechanism is employed to enhance the security.

Proposed Framework

- **Dual CAE model training:** encoders and decoders learn non-linear mappings between images and vectors in binarized latent spaces.
- **Joint mapping**: the secret image is encoded and input into a chaotic mapping system with the vector of the container image, outputing a secret key. And the container image is transmitted to receiver with the secret key.
- **Recovering CAE training**: the container image is encoded and mapped with the secret key to recover the secret image via decoder.
- **Refining U-Net training:** a Refining U-Net is trained to further improve the image quality.

Experimental Results

- Results of **subjective comparison** indicate both the best imperceptibility and reconstruction quality of J-CAE, as shown in Figure 2.
- Pixel error, PSNR, and SSIM are employed for the **objective evaluation** as shown in Table 1. Our J-CAE obtains the lowest pixel error and the highest PSNR and SSIM in both cover and hidden images.
- StegExpose is used for **security analysis via** ROC curves (Figure 3). The AUC value of our method is 0.55 indicating the difficulty to correctly identify container images of J-CAE. In addition, our AUC value is smaller than the values of other three methods [1,10,12], which are 0.62, 0.58 and 0.56.

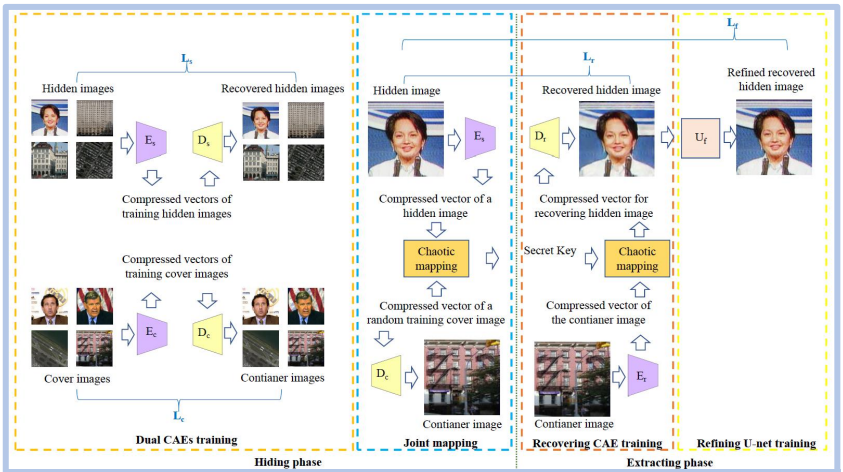

Figure 1: Overall framework of our proposed J-CAE

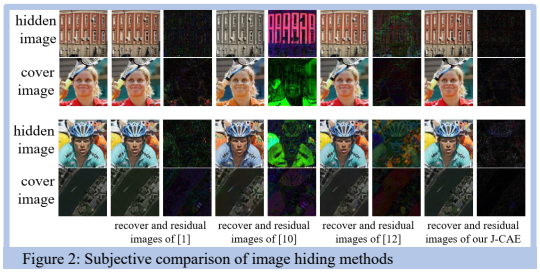

Figure 2: Subjective comparison of image hiding methods

	Baluja *et al.* [1]	Wu *et al.* [10]	Duan *et al.* [12]	J-CAE
cover image				
pixel error	3.1012	4.4224	2.8302	**1.7881**
PSNR	31.7526	29.7046	37.3406	**40.4039**
SSIM	0.9704	0.9653	0.9893	**0.9921**
hidden image				
pixel error	2.9329	7.4876	5.5404	**1.9547**
PSNR	34.2448	27.2817	31.9353	**39.5338**
SSIM	0.9731	0.9458	0.9728	**0.9890**

Table 1: Objective comparation of image hiding methods

Conclusion

We propose **J-CAE** for full-image-to-image hiding based on joint compressive autoencoders, which can achieve both high hidden capacity and better recovery quality of secret images. Our method also achieves better imperceptibility by mapping representations. Experimental results have demonstrated that J-CAE outperforms other three existing DL-based full-image-to-image hiding methods based on both subjective and objective comparisons, also securer.

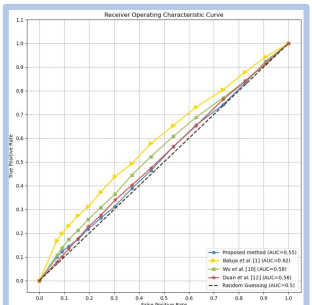

Figure 3: The ROC Curve

[1] S. Baluja, "Hiding images within images," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 42, no. 7, pp. 1685–1697, 2019.
[10] P. Wu, Y. Yang, and X. Li, "Stegnet: Mega image steganography capacity with deep convolutional network," Future Internet, vol. 10, no. 6, p. 54, 2018.
[12] X. Duan, K. Jia, B. Li, D. Guo, E. Zhang, and C. Qin, "Reversible image steganography scheme based on a u-net structure," IEEE Access, vol. 7, pp. 9314–9323, 2019.