A Novel Image Steganography Method via Deep Convolutional Generative Adversarial Networks

Shi Zhiyuan 2020171120@mail.hfut.edu.cn

Introduction

Image steganography is the art and science of hiding secret information in a carrier image so that a receiver can recover the secret information while a warder cannot detect the presence of the secret information. Currently, most image steganography methods achieve the goals of steganography by embedding secret information into carrier images, which unavoidably leaves evidence of distortion. Steganalysis algorithms are developed to determine whether an image has been embedded based on statistical features of distortion.

Adaptive steganography algorithms are proposed to minimize the embedding distortion by using syndrome-trellis codes; however, they can also be detected by more advanced machine-learning-based steganalysis algorithms, such as rich models and deep-learning-based methods . To further reduce the risk of being detected by steganalyzer, scholars have proposed the novel concept of steganography without embedding (SWE) .

Main idea

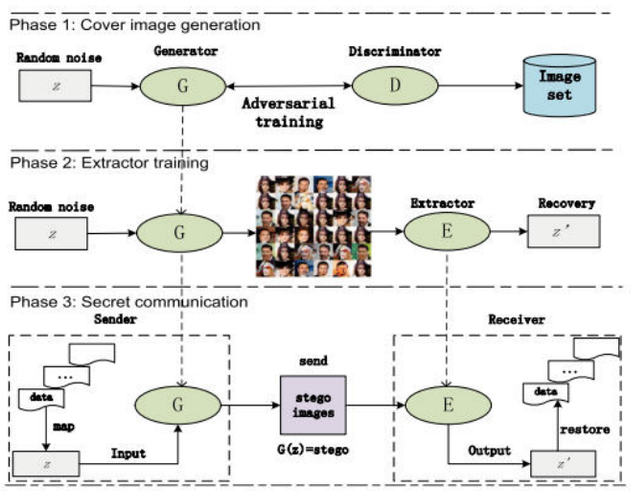

FIGURE 1. The proposed steganography framework using DCGANs for SWE.

As illustrated in Fig. 1, the proposed steganography framework consists of three phases. In first phase, we train DCGANs on an image set and obtain generator G after DCGANs convergence. The network parameters of G are determined after the first phase, and the cover images are produced by G. During the second phase, we train a CNNs model, called the extractor E, based on the recovery errors from a large number of random noise vectors. We use G to extract information from stego images produced by G. In the third phase, the sender and the receiver hold the network and parameters of G and E, respectively. The sender divides the secret information into segments Si, maps the segments into vectors zi, and generates stego images by G according to z. After the receiver receives the stego images, who uses E to extract vector z0 i and then restores the secret data from z0i. The main notation used in this section is given in Table 2.

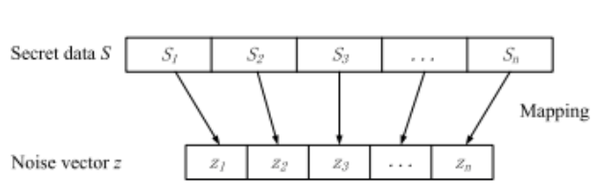

FIGURE 2. Diagram of mapping secret data into vectors.

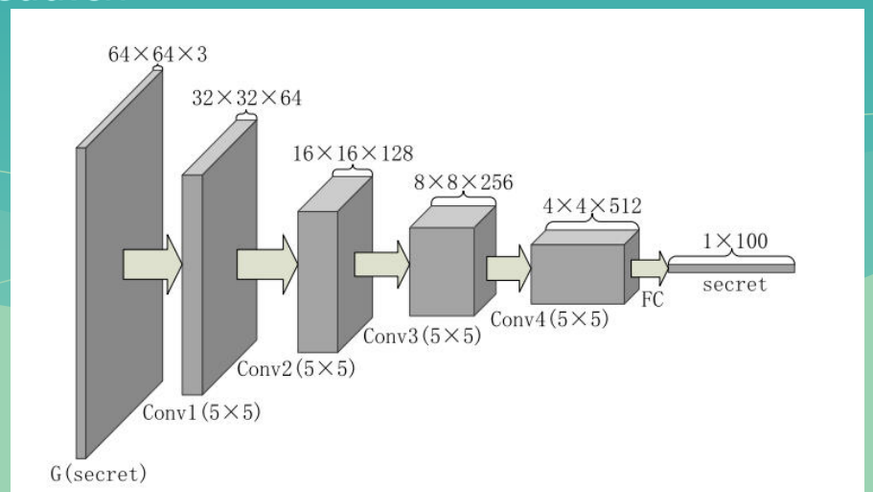

FIGURE 3. The structure of extractor E.

Conclusion

This paper proposes a new image steganography method based on stego images generated by DCGANs according to secret information. In other words, we build a functional relationship between secret information and stego images without embedding by using CNNs. Moreover, CNNs model that can successfully extract secret information from stego images is proposed. The imperceptibility of secret information by this method is significantly improved such that the image steganography can effectively resist detection by steganalysis and forensics algorithms. We apply DCGANs to image

References

[1] C. Cachin, ‘‘An information-theoretic model for steganography,’’ in Information Hiding. Berlin, Germany: Springer, 1998, pp. 306–318. [Online].

Available: https://doi.org/10.1007/3-540-49380-8_21