

INTISARI

Dalam era digital yang terus berkembang ancaman terhadap privasi dan kerahasiaan data semakin meningkat, terutama serangan siber seperti pencurian data dan manipulasi informasi. Steganografi dapat menjadi solusi untuk menjaga kerahasiaan data dengan menyembunyikan pesan dalam gambar. Namun, perkembangan teknik steganalisis yang canggih menyulitkan keberhasilan steganografi, terutama menggunakan metode steganografi yang umum. Penelitian ini mengusulkan penggunaan algoritma deep learning, khususnya arsitektur Generative Adversarial Network (GAN), untuk meningkatkan keamanan steganografi. Metode ini melibatkan penggunaan SRGAN (Super Resolution GAN) untuk meningkatkan resolusi gambar cover sehingga dapat menampung lebih banyak pesan dan tidak terdeteksi pada alat steganalisis. Proses steganografi pada proses implementasi menggunakan metode Least Significant Bit (LSB) dan pengujian steganalisis menggunakan aplikasi StegSpy. Hasilnya dengan mengukur nilai SSIM, PSNR dan RMSE dari tiap gambar, didapatkan rerata nilai SSIM dan PSNR yang meningkat. Pada gambar Low Resolution, mendapatkan rata-rata nilai SSIM = 0,99992233 dan PSNR = 63,833 serta RMSE = 0,000365. Sedangkan pada gambar stego hasil generate model SRGAN mendapatkan rerata nilai SSIM = 0,99992043 dan PSNR = 67,821 serta RMSE = 0,000914 dengan panjang pesan rahasia 1329 karakter. Pada pesan rahasia 207 karakter rerata nilai SSIM dan PSNR meningkat cukup besar dengan nilai rerata SSIM = 0,99999109 dan PSNR = 75,804 dan untuk RMSE didapatkan nilai yang sama dengan gambar Low Resolution. Untuk proses pendeteksian steganografi pada aplikasi StegSpy didapatkan semua gambar tidak terdeteksi pada aplikasi tersebut. Secara umum, dapat disimpulkan bahwa dengan meningkatkan kualitas gambar menggunakan model SRGAN dapat meningkatkan kualitas pada gambar stego dan tidak terdeteksi pada alat steganalisis.

Kata kunci: Super Resolution, Generative Adversarial Network, Steganografi, Least Significant Bit, Steganalisis

ABSTRACT

In the evolving digital era, the threats to data privacy and confidentiality are increasing, especially cyber-attacks such as data theft and information manipulation. Steganography can be a solution to maintain data confidentiality by hiding messages in images. However, the development of sophisticated steganalysis techniques makes it difficult for steganography to succeed, especially using common steganography methods. This research proposes the use of deep learning algorithms, specifically the Generative Adversarial Network (GAN) architecture, to improve the security of steganography. This method involves the use of SRGAN (Super Resolution GAN) to increase the resolution of the cover image so that it can hold more messages and not be detected in the steganalysis tool. The steganography process in the implementation process uses the Least Significant Bit (LSB) method and steganalysis testing using the StegSpy application. The results by measuring the SSIM, PSNR and RMSE values of each image, obtained the average SSIM and PSNR values that increase. In the Low Resolution image, getting the average value of SSIM = 0.99992233 and PSNR = 63.833 and RMSE = 0.000365. While in the stego image the results of the SRGAN model generate the average value of SSIM = 0.99992043 and PSNR = 67.821 and RMSE = 0.000914 with a secret message length of 1329 characters. In the secret message of 207 characters, the average value of SSIM and PSNR increases considerably with an average value of SSIM = 0.99999109 and PSNR = 75.804 and for RMSE, the same value is obtained as the Low Resolution image. For the steganography detection process in the StegSpy application, all images are not detected in the application. In general, it can be concluded that by improving the image quality using the SRGAN model can improve the quality of the stego image and not detected in the steganalysis tool.

Keywords: Super Resolution, Generative Adversarial Network, Steganography, Least Significant Bit, Steganalysis