عنوان مقاله:

Checking The Authenticity and Security of Files and Images ProducedBased on Artificial Intelligence Models

محل انتشار:

بیست و یکمین کنفرانس ملی علوم و مهندسی کامپیوتر و فناوری اطلاعات (سال: 1402)

تعداد صفحات اصل مقاله: 38

نویسندگان:

AmirAbbas Ranjbar
Alireza Chamkoori
Reza Mashayekhi
Peyman Arebi
Sajed Mohisan
Karim Dameshgh

خلاصه مقاله:

The widespread utilization of Artificial Intelligence (AI) models, such as Generative AdversarialNetworks (GANs), has demonstrated remarkable achievements in the field of image synthesis. The proliferation ofAI-generated images, created through GANs, has become prevalent on the Internet due to advancements ingenerating realistic and lifelike visuals. While this development has the potential to enhance content and media, italso poses threats in terms of legitimacy, authenticity, and security. Consequently, it is crucial to develop anautomated system capable of identifying and distinguishing between GAN-generated images and real ones, servingas an evaluation tool for image synthesis models, regardless of the input modality. To address this issue, we proposea framework that utilizes Convolutional Neural Networks (CNNs) to reliably detect AI-generated images fromauthentic ones. Initially, we collected a diverse set of GAN-generated images from various tasks and architectures toensure the model's generalizability. Subsequently, transfer learning was implemented, followed by the integration ofseveral Class Activation Maps (CAM) to identify the discriminative regions that guide the classification model inmaking decisions. Our approach achieved a ۱۰۰% accuracy on our dataset, which consisted of Real or SyntheticImages (RSI), and demonstrated superior performance on other datasets and configurations. Thus, our frameworkcan serve as an effective evaluation tool for image generation. Our most successful detector was an EfficientNetB۴model, pre-trained on our dataset, fine-tuned with a batch size of ۶۴ and an initial learning rate of ۰.۰۰۱ for ۲۰epochs. We utilized the Adam optimizer and incorporated learning rate reduction techniques and data augmentationto further improve performance

کلمات کلیدی:

Performance, Dataset, Synthetic