Investigating Image Steganalysis and Steganography in Digital Forensics based on Convolutional Neural Network

Submitted By

Mohammad Hazem Ghulam

Supervisor By

Dr. Hussam Mustafa

Abstract

Steganography has been used to conceal sensitive data against unauthorized attempts to reveal it since ancient times. However, the development of digital media shows that terrorism and child pornography have both exploited steganography as a tactic. In light of this context, steganography's countermeasure is steganalysis. The two primary schools of steganalysis are universal, sometimes known as blind, and specific. This study investigates image steganalysis and steganography in digital forensics using Convolutional Neural Networks (CNNs). CNNs have shown a good performance in computer vision tasks, and the aim is to develop precise tools for detecting concealed information from various steganographic approaches. A systematic approach involving training, evaluation, and analysis aims to enhance the understanding and capabilities of steganalysis techniques using CNNs. This thesis explores digital crime and its challenges, including identity theft, online piracy, hacking, and

cyberterrorism. Information technology advancements have improved quality of life but also opened up new opportunities for criminals. The research also examines the role of digital forensics in combating cybercrime and the ongoing need for innovative methods and tools. By investigating the capabilities of Convolutional Neural Networks in image steganalysis and considering the broader landscape of digital crime and anti-forensics, this study aims to contribute to the development of more robust and effective tools for digital forensics practitioners. The results demonstrated that our CNN-based technique achieved the highest accuracy of 86%, F1 score of 0.856, a recall of 0.879, a precision of 0.846, outperforming the other algorithms.

Keywords: Steganography, steganalysis, digital forensic, Convolutional Neural Networks (CNNs).

التحقق من إخفاء الصور والمعلومات في الادلة الجنائية الرقمية باستخدام الشبكة العصبونية التلافيفية

إعداد

محمد حازم غلام

إشراف

الدكتور حسام مصطفى

الملخص

تم استخدام علم تحليل الصور لإخفاء البيانات الحساسة ضد المحاولات غير المصرح بها للكشف عنها منذ العصور القديمة. ومع ذلك ، مع تطور وسائل الإعلام الرقمية يظهر أن القراصنة قد استغلوا علم إخفاء المعلومات كتكتيك. ومن خلال هذا السياق ، فإن الإجراء المضاد في علم إخفاء المعلومات هو تحليل الإخفاء. تبحث هذه الدراسة في تحليل إخفاء الصور وإخفاء المعلومات في الادلة الجنائية الرقمية باستخدام الشبكات العصبية التلافيفية (CNNs). أظهرت الشبكات العصبية التلافيفية أداءً جيدًا في مهام رؤية الكمبيوتر ، والهدف من ذلك هو تطوير أدوات دقيقة للكشف عن المعلومات المخفية من مختلف مناهج إخفاء المعلومات. يهدف النهج المنهجي الذي يتضمن التدريب والتقييم والتحليل إلى تعزيز فهم وقدرات تقنيات تحليل الإخفاء باستخدام الشبكات العصبية التلافيفية. تستكشف هذه الرسالة الجريمة الرقمية وتحدياتها ، بما في ذلك سرقة الهوية والقرصنة عبر الإنترنت والقرصنة والإرهاب الإلكتروني. أدت التطورات في مجال تكنولوجيا المعلومات إلى تحسين نوعية الحياة ، ولكنها أتاحت أيضًا فرصًا جديدة للمجرمين. يدرس البحث أيضًا دور الأدلة الجنائية الرقمية في مكافحة الجرائم الإلكترونية والحاجة المستمرة لأساليب وأدوات

مبتكرة. من خلال التحقيق في قدرات الشبكات العصبية التلافيفية في تحليل إخفاء الصور والنظر في المشهد الأوسع للجريمة الرقمية ، تهدف هذه الدراسة إلى المساهمة في تطوير أدوات أكثر قوة وفعالية لممارسي الادلة الجنائية الرقمية .

الكلمات المفتاحية: علم اخفاء البيانات ، تحليل اخفاء البيانات ، الادلة الجنائية الرقمية ، الشبكات العصبية التلافيفية (CNNs).