


Latest Trends in Deep Learning Techniques for Image Steganography


Vijay Kumar, Dr. B.R. Ambedkar National Institute of Technology, Jalandhar, India*

Sahil Sharma, Jaypee University of Information Technology, India

 <https://orcid.org/0000-0002-6694-3365>

Chandan Kumar, Amrita Vishwa Vidyapeetham, Amaravati, India

Aditya Kumar Sahu, Amrita Vishwa Vidyapeetham, Amaravati, India

 <https://orcid.org/0000-0003-4257-0688>

ABSTRACT

The development of deep convolutional neural networks has been largely responsible for the significant strides forward made in steganography over the past decade. In the field of image steganography, generative adversarial networks (GAN) are becoming increasingly popular. This study describes current development in image steganographic systems based on deep learning. The authors' goal is to lay out the various works that have been done in image steganography using deep learning techniques and provide some notes on the various methods. This study proposed a result that could open up some new avenues for future research in deep learning based on image steganographic methods. These new avenues could be explored in the future. Moreover, the pros and cons of current methods are laid out with several promising directions to define problems that researchers can work on in future research avenues.

KEYWORDS

Container Image, Cover Image, Deep Learning, Information Hiding, Secret Image, Steganalysis, Steganography

1. INTRODUCTION

Steganography refers to hiding secret information inside some cover, and steganalysis refers to recovering the secret information. Steganography has been around for thousands of years. The word steganography roughly translates to secret writing. Since the first modern human settlements, there has been a demand for private and secure communication channels so that one person can send a message to another so that no one else can know that the message even exists. In the past, most secret messages were military-related; therefore, no one needed to discover the presence of the message. As the danger of discovery was great, they used various extreme methods like writing messages on

DOI: 10.4018/IJDCF.318666

*Corresponding Author

This article published as an Open Access article distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0/>) which permits unrestricted use, distribution, and production in any medium, provided the author of the original work and original publication source are properly credited.

someone's scalp and then waiting for hair to grow up and hide the message, writing the message on silk and then compressing it into a ball covered with wax and writing the messages on wooden tables and covering them with wax.

In more recent history, during world wars, Nazis used microfilm chips the size of a standard typewriter that could hold pages worth of information, drawings, etc. Some used invisible inks, null ciphers, and many other methods.

With the exponential growth of the internet and the world wide web in the last decades, there are a lot of questions and worries about users' privacy. Personal private information of users is being stolen, spread, snooped on, and so on. The demand for steganography is now more than ever. We no longer have to fear tyrant kings and cruel military personnel, but that doesn't solve the problem. Now we have multinational companies recording our every activity over the internet, and there's also the problem of random bad actors trying to get our personal information. With so much private data being created daily, it could negatively affect people's lives if it falls into the wrong hands (Kerry, 2018). There's an urgent need for Information hiding, and researchers are taking notice. Steganography has become one the most popular methods for information hiding because of its simplicity and easy communication through already existing technology and communication channels like IP cameras, smartphones, and social media apps like WeChat, WhatsApp, Telegram, Signal, etc. without any extra cost of additional infrastructures like private key sharing or private communication channels, etc. There have been various works which have not included deep learning in their work, however, have contributed in the field of watermarking and steganography (Hassaballah *et al.*, 2020; Gutub and Al-Ghamdi, 2020; Gutub and Al-Roithy, 2021; Hassan and Gutub, 2021; Al-Roithy and Gutub, 2021; AlKhodaidi and Gutub, 2021; Hameed, Abdel-Aleem and Hassaballah, 2022; Gutub, 2022a, 2022b).

With the rise of deep learning algorithms, steganography has also taken a step forward. Various deep learning algorithms provide a better, more efficient approach to achieving the desired results. But the rise of deep learning has also been counterintuitive to achieving reliable and robust image steganography results since there are just as many deep learning-based steganalysis algorithms. Steganography and steganalysis play a push-and-pull game. Because of the recent improvements in the steganalysis algorithms using deep learning, it is imperative that the steganographic techniques also catch up and provide better robust and reliable results that can avoid steganalysis.

There are basic Image steganography techniques that have been around for some time. Like the Least Significant Bit (LSB) encoding steganography in which the least significant overwritten by the secret message bits or the Masking and Filtering technique in which watermarks are inserted on top of grayscale or RGB Images or the Shift encoding techniques like the Line Shift Coding and Word Shift Coding. A few of these techniques work well under certain circumstances. Hinton and Salakhutdinov (Hinton and Salakhutdinov, 2006) worked on unsupervised pre-training methods proposing optimization of the initial network weight values and then fine-tuning the weights. It is considered the starting point of using deep learning algorithms in steganography. Much research and experimentation took place after that, and various deep-learning algorithms revolutionized the Steganography process. They work exceptionally well than the basic methods as they have certain advantages and problems over the basic techniques, as discussed in the following sections (Hiwe and Nipanikar, 2014).

This paper lays out a comprehensive review of various deep learning algorithms used or could be used in achieving Image Steganography. Different tactical foundations of image steganographic methods are analyzed to rank and review their performances, strengths, and shortcomings.

The contributions of the current work are as follows:

1. To discuss the deep learning-based works in the field of image steganography.
2. To present the comparative analysis of various techniques.
3. To discuss the literature about GANs, Autoencoders, Reinforcement Learning, Attention-based models, and CNNs.
4. To present the future research directions.

12 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/article/latest-trends-in-deep-learning-techniques-for-image-steganography/318666

Related Content

Predicting Future Cybercrime Trends in the Metaverse Era

Wasswa Shafik (2024). *Forecasting Cyber Crimes in the Age of the Metaverse* (pp. 78-113).

www.irma-international.org/chapter/predicting-future-cybercrime-trends-in-the-metaverse-era/334496

A Forensic-as-a-Service Delivery Platform for Law Enforcement Agencies

Fabio Marturana, Simone Tacconiand Giuseppe F. Italiano (2013). *Cybercrime and Cloud Forensics: Applications for Investigation Processes* (pp. 313-330).

www.irma-international.org/chapter/forensic-service-delivery-platform-law/73968

Dental Age Assessment (DAA) of Children and Emerging Adults: A Practical Guide

Graham J. Robertsand Aviva Petrie (2011). *Digital Forensics for the Health Sciences: Applications in Practice and Research* (pp. 226-279).

www.irma-international.org/chapter/dental-age-assessment-daa-children/52291

Android Adware Detection Using Machine Learning

Sikha Baguiand Daniel Benson (2021). *International Journal of Cyber Research and Education* (pp. 1-19).

www.irma-international.org/article/android-adware-detection-using-machine-learning/281679

Telecommunications Interception in Turkey: Rights to Privacy vs. Discourses of Security

Melike Akkaraca Köse (2012). *Cyber Crime: Concepts, Methodologies, Tools and Applications* (pp. 790-813).

www.irma-international.org/chapter/telecommunications-interception-turkey/60982