ScienceDirect

Journal of Visual Communication and Image Representation

Volume 60, April 2019, Pages 266-275

Research on image steganography analysis based on deep learning ☆

Ying Zou [a] ✉, Ge Zhang [b c] ✉, Leian Liu [a] ✉

Show more

Share Cite

https://doi.org/10.1016/j.jvcir.2019.02.034 ↗

Get rights and content ↗

Abstract

Although steganalysis has developed rapidly in recent years, it still faces many difficulties and challenges. Based on the theory of in-depth learning method and image-based general steganalysis, this paper makes a deep study of the hot and difficult problem of steganalysis feature expression, and tries to establish a new steganalysis paradigm from the idea of feature learning. The main contributions of this paper are as follows: 1. An innovative steganalysis paradigm based on in-depth learning is proposed. Based on the representative deep learning method CNN, the model is designed and adjusted according to the characteristics of steganalysis, which makes the proposed model more effective in capturing the statistical characteristics such as neighborhood correlation. 2. A steganalysis feature learning method based on global information constraints is proposed. Based on the previous research of steganalysis method based on CNN, this work focuses on the importance of global information in steganalysis feature expression. 3. A feature learning method for low embedding rate steganalysis is proposed. 4. A general steganalysis method for multi-class steganography is proposed. The ultimate goal of general steganalysis is to construct steganalysis detectors without distinguishing specific types of steganalysis algorithms.

Introduction

With the rapid development of information technology and the rapid popularization of the Internet, digital media has become an important carrier for military, commercial and other organizations as well as individuals to obtain and transmit information. But at the same time, because the digital communication in the Internet is vulnerable to the threat of eavesdropping,

malicious interference and other activities, people pay more attention to the security issues such as privacy protection and data integrity in the process of information transmission than ever before. The traditional solution uses encryption technology to convert the information to ciphertext for transmission. But its shortcoming is that the encrypted ciphertext is usually disordered. It is easy for an attacker to notice the existence of secret communication, which stimulates the attacker's enthusiasm for decoding. At the same time, it may also lead to information being interfered or intercepted, resulting in the failure of information transmission. In the above context, a new concept of communication security has been gradually accepted and recognized: communication security means not only that the content of information to be transmitted is secure, but also that the existence of the act of transmitting secret information is unknown. Therefore, steganography, which is characterized by “camouflage” in the transmission of information, has attracted more and more attention.

The basic principle of steganography is to hide the secret information which needs to be transmitted into the redundant information by using the insensitive redundant information of human perception system existing in common carriers, and to realize the transmission of secret information by means of carrier transmission. Because the process of information hiding into the carrier usually does not change the normal perception characteristics of the carrier, it is difficult for potential attackers to detect the existence of secret information, thus ensuring the information security covert transmission. At the same time, it can also combine encryption, scrambling, coding and other technologies, making it difficult to extract hidden information even if it is detected by third parties, thus further ensuring the security of information transmission. In order to explain steganography more vividly, we describe the “prisoner problem” as an example. Alice and Bob are prisoners in different cells in the same prison. They are under the care of Warden Eve. Alice and Bob are going to discuss plans for a joint jailbreak. Specific plans need to be negotiated through the exchange of information. However, according to prison regulations, their communications need to be checked by the warden, so they cannot communicate in plaintext. In this case, Bob and Mice need to take more covert communication measures. One consideration is to use encryption technology, that is, to hide the content of information, but because the encrypted information is a mess of code, it is easy to arouse Eve's suspicion. Thus, in this case, a safer consideration is to hide information in everyday objects, and make the hidden objects look normal, which can reduce Warden Eve's vigilance and ensure the smooth transmission of information.

However, steganography is also a true double-edged sword, which provides people with reliable and secure means of Internet communication, at the same time, it may also provide convenience for organizations and individuals with malicious intentions or improper purposes [11], [12], [13], [14]. In fact, in recent years, there have been reports about the use of steganography in espionage, terrorist attacks, crimes and other activities. In 2001, some mainstream media in the United States, such as CNN and US Today, reported the news of secret communications between Al Qaeda members using steganography. Reported that bin Laden gang will attack the target map, action instructions and other information hidden in pornography, sports chat and other websites. According to Die Zeit, an al-Qaida suspect was arrested in Berlin in May 2011 and police found him carrying a memory card. Later, after being cracked by experts in charge of computer criminal

investigation in the German Federal Criminal Police Bureau, it was found that on the surface, only one pornographic video named “KickAss” appeared on the card, but in fact, 141 text documents were hidden in the video, including a large number of Al-Qaida action reports, future action plans and so on. In June 2010, the Federal Bureau of Investigation (FBI) successfully arrested 10 Russian agents in New Jersey, which caused a great diplomatic shock between the United States and Russia.

The FBI said that by eavesdropping on the conversations between the Murphy couple, who were all suspects, they found that Murphy had sent his wife Cynthia to South America to hand over something “invisible” to someone. According to the FBI analysis, these so-called “invisible things” are likely to be recorded by digital steganography. They also claimed to have found devices for digital steganography in the homes of three suspected Russian agents, and inferred that Russian agents used steganography to communicate information with relevant Russian intelligence agencies. According to a Reuters report in July 2015, a report released by security manufacturer FireEye shows that Russian hackers have successfully invaded the U.S. defense system and captured several computers of the U.S. Department of Defense using data from Twitter that appears to be ordinary photos. These seemingly ordinary Twitter images hide information and instructions to activate malicious programs that have been implanted into the target computer. With the help of the camouflage of Twitter pictures, the transmission of commands controlling malicious programs easily avoids the detection of most detection systems. In April 2014, mainstream media in China, such as CCTV and Xinhua News Agency, reported that the mobile Trojan Horse “immortal Trojan Horse II” infected millions of mobile phones, and carried out fishing attacks, remote control of users' mobile phone photos, stealing users' online silver and other activities that seriously endangered users' personal privacy and property security. It is reported that, unlike the normal Trojan horse direct command mode, the Trojan horse cunningly disguises malicious code instructions as a common picture through steganography, in order to avoid the “pursuit” of mobile phone security software [1], [2], [3], [4], [5], [6], [7], [8], [8], [9], [10].

It can be seen from above that illegal or malicious use of digital steganography has brought serious harm to national information security, business and personal privacy and property security [15], [16], [17], [18], [19]. In this case, how to effectively supervise the use of steganography in real life, prevent or block the malicious or illegal use of steganography in real time has become an urgent need of military and security departments in various countries. Because of this, Steganalysis, as a countermeasure technology of steganography, came into being, and has attracted the attention of governments and scientific research institutions. Steganalysis is a technique to determine whether there is additional information hidden in the carrier or not, even to estimate the amount of information embedded in the carrier, and to obtain the content of the hidden information by analyzing the statistical characteristics of the carrier. It plays the role of Warden Eve in the model of “prisoner problem” mentioned above. The research of steganalysis technology is of great significance in preventing the leakage of confidential information, combating terrorism and criminal activities, and maintaining Internet security.

Based on the theory of in-depth learning method and image-based general steganalysis as the research object, this paper focuses on the hot and difficult problem of feature expression in

steganalysis, and tries to establish a new framework of steganalysis from the new idea of feature learning. The specific research contents of this paper mainly include the following aspects:

1. A digital image steganalysis framework based on depth learning is proposed.

Aiming at the problems in steganalysis, especially in feature expression. Considering feature learning, a new steganalysis paradigm based on in-depth learning is proposed. Based on the representative deep learning method CNN, the proposed model is designed and adjusted according to the characteristics of steganalysis, which makes the proposed model more effective in capturing the statistical characteristics such as neighborhood correlation Related to steganalysis, and automatically expresses the features of steganalysis effectively through learning. Different from traditional methods based on artificial design features, this method integrates feature extraction module and classification module into a trainable network model framework, and automatically learns features and realizes classification in the form of data-driven, thus greatly reducing the need for human experience and time. On this basis, the detection performance is further improved by model fusion and other methods.

2. A steganalysis feature learning method based on global statistical information constraints is proposed.

This work focuses on the importance of global information in steganalysis feature expression, and introduces how to use global statistical information to make the model learn better feature expression under the framework of feature-based learning steganalysis. Referring to the idea of transfer learning, this paper proposes a CNN model based on global statistical information constraints. By calculating auxiliary features to obtain additional global statistical information, and then introducing global statistical information into CNN model in the form of auxiliary tasks in migration learning, regularization constraints are applied to training CNN model, so that it can learn better feature expression.

3. A feature learning method for low embedding rate steganalysis is proposed.

In the field of steganalysis, the detection of low embedding rate encrypted images is a key concern. The difficulty lies in the small amount of embedding information, which makes the change of image statistical characteristics relatively small, so it is more difficult to detect. To solve this problem, based on the idea of Transfer Learning, this paper proposes to enhance the feature learning on low embedding rate dense image datasets by migrating the prior information of features learned from high embedding rate dense image datasets of CNN, so as to improve the detection performance of CNN model for low embedding rate dense image.

4. A general steganalysis method for multi-class steganography is proposed.

From the current research status of general steganalysis algorithms, the “universality” of existing methods only reflects that different steganalysis algorithms can use the same algorithm steps to

construct detectors. However, in the process of constructing the detector, we need to know the specific types of edge information of the steganography algorithm to be detected, and use these edge information to generate the dense image for training. There are many possible steganography algorithms in real application scenarios. Steganalysts often find it difficult to know which steganography users use. Therefore, it is urgent and significant to study steganalysis detectors for different steganalysis algorithms (known or even unknown). This chapter will explore this issue. On the basis of previous research on Steganalysis Based on in-depth learning and combined with the idea of multi-task learning, this paper tries to propose a steganalysis method for steganographic images generated by different steganographic algorithms.

Access through your organization

Check access to the full text by signing in through your organization.

Access through your organization

Section snippets

Relevant research summary

Neil E. Johnson of George Mason University in the late 1990s in the United States first began the study of steganalysis. Later, Dartmouth College, Massachusetts Institute of Technology, New York State University, Purdue University, New Jersey Institute of Technology, Wet Stone Corporation, IBM Corporation, Microsoft Corporation and other institutions have carried out research in this direction, and most of them have received strong support from the United States Department of Defense, the …

Summary

With the rapid development and popularization of computer and Internet technology, the problem of information security on the network has become increasingly prominent. Steganography, as a representative covert communication technology, can be used illegally by terrorist organizations, spies and criminal gangs while ensuring communication security, thus endangering national security, public and personal privacy security and other issues. Therefore, the research of steganalysis technology for …

Declarations

Ethical Approval and Consent to participate: Approved.

Consent for publication: Approved.

Availability of supporting data: We can provide the data. …

Competing interests

These no potential competing interests in our paper. And all authors have seen the manuscript and approved to submit to your journal. We confirm that the content of the manuscript has not been published or submitted for publication elsewhere. …

Author's contributions

All authors take part in the discussion of the work described in this paper. The author Ying Zou wrote the first version of the paper, and did part experiments of the paper, Ge Zhang initiated the project. Leian Liu revised the paper in different version of the paper. …

Conflict of interest

There is no conflict of interest. …

Funding

This work was supported by the Science and Technology Planning Project of Guangdong Province under Grant (2017A070709012), the quality resource sharing course project-"Computer Network" (Official document by Department of education of Guangdong province ([2015] no. 133)), the provincial-level characteristic specialty-"Network Engineering" and the provincial teaching team-"Teaching team of basic core course of computer major" (Official document by Department of education of Guangdong province …

Acknowledgements

The authors thank the editor and anonymous reviewers for their helpful comments and valuable suggestions. …

Ying Zou was born in Henan, china in 1979. She is currently a lecturer in Zhongkai University of Agriculture and Engineering, China. She is a member of China Computer Federation. Her research interests include: network security technology, IoT technology and machine learning. In recent five years, as the first author has published 1 paper, chaired three software copyrights. …

…

…

Recommended articles

References (23)

Abbas Cheddad
Digital image steganography: survey and analysis of current methods
Signal Process. (2010)

Chang-Chou Lin *et al.*
Secret image sharing with steganography and authentication
J. Syst. Software (2004)

Neil F. Johnson *et al.*
Exploring steganography: seeing the unseen.
Computer (1998)

Jessica Fridrich *et al.*
Detecting LSB steganography in color, and gray-scale images
IEEE Multimedia (2001)

L. Zhang *et al.*
Probabilistic graphlet cut: exploiting spatial structure cue for weakly supervised image segmentation.

Cachin, Christian, An information-theoretic model for steganography, International Workshop on Information Hiding,...

Lisa M. Marvel *et al.*
Spread spectrum image steganography
IEEE Trans. Image Process. (1999)

Donovan Artz
Digital steganography: hiding data within data
IEEE Int. Comput. (2001)

Junwei Han *et al.*
Object detection in optical remote sensing images based on weakly supervised learning and high-level feature learning
IEEE Trans. Geosci. Remote Sens. (2015)

Weiqi Luo *et al.*
Edge adaptive image steganography based on LSB matching revisited
IEEE Trans. Inform. Forensics Secur. (2010)

View more references

Cited by (35)