Authorship Analysis in Cybercrime Investigation

Rong Zheng, Yi Qin, Zan Huang, and Hsinchun Chen

Artificial Intelligence Lab
Department of Management Information Systems
The University of Arizona
Tucson, Arizona 85721, USA
{rong, yiqin, zhuang, hchen}@eller.arizona.edu

Abstract. Criminals have been using the Internet to distribute a wide range of illegal materials globally in an anonymous manner, making criminal identity tracing difficult in the cybercrime investigation process. In this study we propose to adopt the authorship analysis framework to automatically trace identities of cyber criminals through messages they post on the Internet. Under this framework, three types of message features, including style markers, structural features, and content-specific features, are extracted and inductive learning algorithms are used to build feature-based models to identify authorship of illegal messages. To evaluate the effectiveness of this framework, we conducted an experimental study on data sets of English and Chinese email and online newsgroup messages. We experimented with all three types of message features and three inductive learning algorithms. The results indicate that the proposed approach can discover real identities of authors of both English and Chinese Internet messages with relatively high accuracies.

1 Introduction

The development of networking technologies, and the Internet in particular, has created a new way to share information across time and space. While computer networks have enhanced the quality of life in many aspects, they have also opened a new venue for criminal activities. These activities have spawned the concept of cybercrime, which refers to illegal computer-mediated activities that can be conducted through global electronic networks, such as the Internet [31]. One predominant type of cybercrime is distribution of illegal materials in cyber space. Such materials include pirate software, child pornography materials, stolen properties, etc.

Cyber criminals have been using various Web-based channels to distribute illegal materials such as Email, websites, Internet newsgroups, Internet chat rooms, etc. One common characteristic of these channels is anonymity. People usually do not need to provide their real identity information, such as name, age, gender, and address, in order to participate in cyber activities. Compared to conventional crimes, cybercrime conducted through such anonymous channels imposes unique challenges for law enforcement agencies in criminal identity tracing. The situation is further complicated by the sheer amount of cyber users and activities, making the manual approach to criminal identity tracing impossible for meeting cybercrime investigation requirements. Law enforcement agencies have an urgent need for approaches that automate...
criminal identity tracing in cyberspace and allow investigators to prioritize their tasks and focus on the major criminals.

In this paper we propose to adopt the authorship analysis framework in the context of cybercrime investigation to help law enforcement agencies deal with the identity-tracing problem. We extract three types of features that are identified in authorship analysis research from online illegal messages and use inductive learning techniques to build feature-based models to perform automatic message author identification. We are specifically interested in evaluating the general effectiveness of this approach and the effects of using different types of features in the cybercrime investigation context. Because of the multinational nature of cybercrime, we are also interested in evaluating the applicability of the proposed framework in a multilingual context.

The remainder of the paper is organized as follows. Section 2 surveys the existing work on authorship analysis and summarizes major types of text features and techniques. Section 3 describes our proposed cyber criminal identity-tracing framework in detail and presents the specific research questions that we aim to address. Section 4 presents an experimental study that answers the research questions raised in Section 3, based on several experimental data sets. We conclude the article in Section 5 by summarizing our research contributions and pointing out future directions.

2 Literature Review

2.1 Authorship Analysis

Authorship analysis is the process of examining the characteristics of a piece of work in order to draw conclusions on its authorship. More specifically, the problem can be broken down into three sub-fields [35]:

- **Author Identification** determines the likelihood of a particular author having written a piece of work by examining other works produced by that author.
- **Author Characterization** summarizes the characteristics of an author and generates the author profile based on his/her work. Some of these characteristics include gender, educational and cultural background, and language familiarity.
- **Similarity Detection** compares multiple pieces of work and determines whether or not they are produced by a single author without actually identifying the author.

Authorship analysis has many applications. It is rooted in the author attribution problem of historical literature. The most famous one is its success in resolving the debate on Shakespeare’s work [10]. Similarly, authorship analysis techniques have assisted in solving the author debates over the Federalist Papers [23] and the Unabomber Manifesto [13]. Another application domain is software forensics [14]. People try to identify or characterize the author of some malicious programs by analyzing executable code or source code to investigate the crime and prevent future attacks. Since our work is mainly concerned with text, we will not discuss software forensics in this paper.

Generally, the major topics on authorship analysis in the past research are feature selection and the techniques used to facilitate the analysis process. In the following sub-section we review the literatures from these two perspectives.