Graph-Based Spam Image Detection for Mobile Phone Spam Image Filtering

So Yeon Kim, Department of Information and Computer Engineering, Ajou University, Suwon, South Korea

Kyung-Ah Sohn, Department of Information and Computer Engineering, Ajou University, Suwon, South Korea

ABSTRACT

Spam images in mobile phones have increasingly appeared these days. As the spam filtering systems become more sophisticated, spams are being more intelligent. Although detection of email-spams has been quite successful, there have not been effective solutions for detecting mobile phone spams yet, especially, spam images. In addition to the expensive image processing time, insufficient spam image data in mobile phones makes it challenging to train a general model. To address this issue, the authors propose a graph-based approach that utilizes graph structure in abundant e-mail spam dataset. The authors employ different clustering algorithms to find a subset of e-mail spam images similar to phone spam images. Furthermore, the performance behavior with respect to different image descriptors of Pyramid Histogram of Visual Words (PHOW) and RGB histogram is extensively investigated. The authors' results highlight that the proposed idea is fairly meaningful in increasing training data size, thus effectively improving image spam detection performance.

Keywords: Color SIFT, Graph Clustering, Image Classification, PHOW, Spam Detection, Spam Image, Spectral Clustering

INTRODUCTION

Image-based spams, or image spams for short, are widely spread in all kinds of media. According to a bunch of personal information leaks, spam messages are increasingly appearing in personal areas like in a smart phone. Although there have been many studies on detecting spam images in e-mails or web pages, those in a mobile phone are much more insufficient than in other media.

There have been several approaches for detecting spam text messages effectively. Those unsolicited spam messages have caused severe social problems in that they are used for bank fraud and financial crimes. In order to avoid the conventional text-based spam filtering system, spam messages have been evolved. They include unnecessary special characters or white spaces.
between words to prevent spam filtering from detecting spam keywords. Usually, spam messages can be detected by user-supplied spam number database. It can be nevertheless deceived by changing their sending number or by using an actual user’s number to be filtered out of the database.

Furthermore, image spams without any text are rapidly increasing in mobile phones these days, thus making spam detection even harder. Due to the high cost of image processing in a mobile phone as well as insufficient phone spam image data, detecting spam images in a mobile phone becomes a difficult issue that we struggle with. Accordingly, researches on phone spam images are quite necessary. However, the size of phone spam image data is still too small to train a predictive model with sufficient accuracy.

In this respect, we propose a phone spam image filtering system taking advantage of widely available e-mail spam image data. As some e-mail spam images look different from phone spam images, we select a visually similar sub-group of e-mail spam images from graph-based clustering techniques. We demonstrate the spam classification performance using the similar subset of e-mail spam images in addition to the phone spam images. Also, we investigate the effectiveness of using the graph structure in e-mail spam data. To obtain similar sub-group of e-mail spam images, graph-based clustering algorithm is used as well as the hierarchical clustering and k-means clustering. In addition, the performance on spam image classification using multiple image descriptors are compared, which are RGB histogram feature and Pyramid Histogram of Visual Words (PHOW) descriptor with gray, RGB, and opponent color mode.

**RELATED WORKS**

Spam filtering algorithm is proposed in many different kinds of media. Especially, spam images are widely spread in e-mail or on the web. Many machine learning approaches are proposed for e-mail spam image filtering (Biggio, Fumera, Pillai, & Roli, 2011; Guzella & Caminhas, 2009). As there is abundant spam text in e-mail and spam filtering system can therefore capture the spam text very well, image spams are rapidly increased. Image analysis such as OCR (Optical Character Recognition) is conducted for embedded images in e-mail (Fumera, Pillai, & Roli, 2006). Rather than computationally expensive OCR processing, many approaches which train the features of spam images are proposed (Aradhye, Myers, & Herson, 2005; Nhung & Phuong, 2007; Wakade, Liszka, & Chan, 2013). For advanced feature extraction techniques, artificial neural networks are used (Soranamageswari & Meena, 2010). In (Al-Duwairi, Khater, & Al-Jarrah, 2011), image texture analysis-based image spam filtering algorithm is newly proposed which uses low-level image texture features. In these works, using image features also showed the desirable performance rather than using expensive OCR techniques.

In (Mahajan & Slaney, 2010), they proposed image spam classification model fusing image, text and web-graph features to handle the spam images on the web. For automatic spam image identification, (Cheng, Deng, Fu, Wang, & Qin, 2011) proposed a graph-based semi-supervised feature selection algorithm to handle redundant features also. It showed that graph features of spam images have positive impact on spam image filtering.

**METHODOLOGY**

**Image Descriptors**

To extract image features, we use existing image descriptors. Each spam or non-spam image is represented by RGB histogram or Pyramid Histogram of Visual Words (PHOW) descriptor

---

Copyright © 2015, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.
The HTTP Flooding Attack Detection to Secure and Safeguard Online Applications in the Cloud
[www.igi-global.com/article/the-http-flooding-attack-detection-to-secure-and-safeguard-online-applications-in-the-cloud/234770?camid=4v1a](www.igi-global.com/article/the-http-flooding-attack-detection-to-secure-and-safeguard-online-applications-in-the-cloud/234770?camid=4v1a)

The Role of Compliance and Conformance in Software Engineering
[www.igi-global.com/chapter/the-role-of-compliance-and-conformance-in-software-engineering/108627?camid=4v1a](www.igi-global.com/chapter/the-role-of-compliance-and-conformance-in-software-engineering/108627?camid=4v1a)