Proceedings of the 2013 International Conference on
Pattern Recognition, Informatics and Mobile Engineering (PRIME) February 21-22

A Study on E-mail Image Spam Filtering Techniques

S. Dhanaraj
Department of MCA
Sree Saraswathi Thyagaraja College
Pollachi, India
sdhanaraj@yahoo.co.in

Dr. V. Karthikeyani
Department of Computer Science
Thiruvalluvar Government Arts College
Rasipuram, India
drvkarthikeyani@gmail.com

***Abstract*—Spam filters are the most used software tool used by businesses and individual to block spam mails entering into their mail boxes. Until recently, majority of research effort was expended on controlling text-based spam emails. However, the past few years have envisaged a novel approach, where the spammers embed the text message into an image. Thus, the anti-spam filtering research is forced to move from text-based techniques to image-based techniques. Spam and the spam blockers designed to combat it have spawned an upsurge in creativity and innovation. Many software developers are developing new and every more effective spam filtering software. All the methods have a common dream that is to eliminate 100% of the spam, which is still not a reality. To reduce the gap between this reality and dream, researchers have proposed many different types of spam filters and this paper provides a review of them.**

Keywords- Spam Filter; Anti-Spam; Image Spam; spam filtering; Anti-Spam Techniques

I. INTRODUCTION

More than 500 million people in the world have Internet access and the popularity of email technology has grown rapidly in recent years. Initially, introduced as a simple electronic communication tool, e-mail has outgrown its origin and become an irreplaceable tool in the today's communication. According to [37], 94% of US Internet users have gone online and sent or read email till May, 2010. The same source suggests that 62% do this as part of daily activities. Another report [51] reports that there are 2.9 billion email accounts in 2010 and is expected to rise to over 3.8 billion by 2014.

Along with the growth in email usage, as an unwanted side effect, viruses, worms and spam (unsolicited mail) have also increased over time. Spam and fraudulent e-mail messages are major issues for Internet users and businesses of all sizes. Companies are being forced to commit significant resources to protect their messaging infrastructure and their brand from these abuses. Spam was once just an annoyance, but it has now become the tactic of choice for online deception, fraud, and abuse. The freedom of communication is being misused and has become a threat to e-mail communication society.

According to Brightmail [6], the percentage of email that is spam is growing consistently and considerably. Similar findings are also reported by another famous antivirus vendor, McCafe, in McAfee Threats Report: Third Quarter 2009. According to this report, spam emails have risen by more than 10 per cent during 2009 when compared to 2008 and spam as a percent of total email volume is more than 92 percent during the same year. This statistics is expected to grow in forthcoming years, which stresses the fact that threats to email communication are increasing at a massive and unchecked pace.

As a solution to the spam problem, several filters were developed to detect or prevent text-based spam mails and are reported to be quite successful in their implementation. Now-a-days, to bypass text based anti-spam filters, some spammers put their spam content into images (i.e. spammers embed text such as advertisement text in the images) and attach these images to emails. The anti-spam filters that analyze content of email cannot detect spam in images [13]. The spam mails embedded with images are termed as "image spam". Image spam is an obfuscating method in which the text of the message is stored as a GIF, JPEG, BMP or PNG image and displayed in the email. This prevents text-based spam filters from detecting and blocking spam messages. Moreover, the recent image spam mails contain animated GIF, which again proves to be a challenge to the existing spam solutions.

Image spam is a phenomenon that appeared during 2005 and by the end of 2006, over 50% of total spam received was image spam. Image spam forms around 12.87% of total email spam which forms around 87.56% of all email [26]. A great deal of on-going research is trying to resolve the image spam problems. This paper reviews and discusses some of the research works done in the field of image anti-spam filters, which detect and prevent image spam into entering the inbox. The remaining sections of the paper are organized as follows. Section 2 gives a brief overview to the concept behind image spam. Section 3 discusses the various proposed image spam filtering techniques. Section 4 presents the various performance parameters used to analyze spam filters. Section 5 consolidates the work with future research directions.

II. IMAGE SPAM – AN OVERVIEW

The action of sending unsolicited commercial messages in bulk quantity with obtaining explicit permission or desire of the recipients is defined as 'Spamming'. The type of spam depends on the medium of communication it is applied on. Examples include email spam, instant messaging spam (spim), Usenet newsgroup spam, web search engines spam, web log spam and mobile phone messaging spam. There are two basic

978-1-4673-5845-3/13/$31.00©2013 IEEE

forms of email spam, Text-based spam mails and Image-based spam mails. Text-based spam mails are emails, consisting of text only message to convey the sender's information. Image-based spam are mails where the spammer's message is sent in the form of a graphic or an image and will be in human readable format. In this paper, "spam" refers to "image spam" and "ham" refers to "legitimate mail". Ham mail can be defined as every email not considered as spam.

Image spam is a technique that spammers use to avoid anti-spam algorithms. All image spam mails follow a common pattern and have a content-free characteristic. It is estimated that maximum of the image spam emails are used to advertise products or services [27], cheat users (either stealing private information or deliver malicious software) or cause temporarily crash of mail servers. An image spam email is formatted in HTML, which usually has only non-suspicious text with an embedded image (sent either as an attachment or via the use of self referencing HTML with image data in its payload). The embedded image carries the target message and most email clients display the message in their entirety. Since, many ham emails also have similar properties (using HTML, carrying embedded images, with normal text) as image-based emails, existing spam filters find it difficult to distinguish between image spam and image ham.

A. *Types of Image Spam*

The Spammer's Compendium provides a compilation of spammer techniques collected and classified by a community of volunteers. According eight classes were identified, namely, text-only images, sliced images, randomized images, color modified images, gray images, wild background images, multi-frame animated images and stock splits [10]. Text-only images appear like a normal text email but in reality, is an image. Sliced images use multiple images combined like a jigsaw puzzle [3]. A spammer usually alters individual pixels in the image that is difficult to distinguish from the original image. Due to the randomization of the pixels, each an iteration of the image will appear completely different to many image spam filters and are termed as randomized images. Due to the unlimited flexibility in the number of colors and fonts, image spammers change the properties of their images resulting in new pixel locations and identifiers and these images are called color modified images.

Gray email is a spam image that could reasonably considered either spam or ham. Handling gray emails is very important issue because they resemble natural gray scale images and should be addressed in spam filtering systems. In wild background images, spammers use high colored and patterned backgrounds, uneven letters, and randomly inserted pixels around the border, which makes it unique and hard to read by any software attempting to use Optical Character Recognition (OCR). Spammers send multiple frames containing an animated GIF image with their message. The frames rotate at a faster rate so that a human eye cannot detect the animation but only watch the final result and are called multi-frame animated images. Stock splits are a new type of image introduced by spammers during 2006, where the original image is split into multiple images, which are reassembled only when the message is opened. This makes it difficult for the filters and image scanning software to detect them.

B. *Types of Spam Content*

According to [41], there are eleven categories of spam, namely, products advertisement, financial, adult, Internet, health, scams, leisure, fraud, political and spiritual.

Email attacks offering or advertising general goods and services are termed as product advertisement spam. Email attacks that contain references or offers related to money, the stock market or other financial opportunities are called financial spam. Adult spam are emails that contain or refer to products or services intended for persons above the age 18, often offensive or inappropriate. Internet spam are mail that specifically offering or advertising Internet or computer related goods and services. Another type of spam attack is the health spam, which offer or advertise health related products and services. Email attacks recognized as fraudulent, intentionally misguiding or known to result in fraudulent activity on the part of the sender are termed as Scams. Email attacks offering or advertising prizes, awards or discounted leisure activities are Leisure spams.

Email attacks that appear to be from a well-known company, but are not. These are known as "brand spoofing" or "phishing", these message are often used to trick users into revealing personal information such as email address, financial information and password. These types of spam mails are called Fraud spam. In a similar fashion, when the email message advertising a political candidate's campaign, which offers to donate money to a party or political cause and also offers for products related to a political figure or campaign, etc., they are called Political spam. Email attacks with the information pertaining to religious or spiritual evangelization and /or services.

III. ANTI SPAM TECHNIQUES

This section presents the techniques and technologies used currently in fighting and blocking spam mails. Many of the techniques presented here have their own strengths and weaknesses and are usually used in combination for maximum effectiveness. Stopping spam exists at several levels and can be broadly categorized as (i) Before spam is sent (ii) After spam is sent (iii) After spam is in mailbox and (iv) Legal solutions.

A. *Before Spam is Sent*

Techniques like Blacklists (block lists) and Whitelists can be used to avoid spam mails. Blacklists as their name implies is a list of people, organizations or companies who have met with the disapproval of others and are prevented from interacting with those who disapprove them. In the online world, a blacklist refers to those people who are responsible for generating spam in a very big way. The blacklisting can be by IP address, person, company or domain. A whitelist is an exact opposite of a blacklist. A whitelist is a predefined list of IP addresses that are allowed to send email to and receive email from each other. To send email to a whitelist, the sender must be approved and verified by the owner of the whitelist. Whitelist reduce server clutters and bandwidth usage

considerably. The benefits of whitelists are many, but proper management of the whitelists is equally important. Misuse of whitelists lead to more difficulties for everyone involved with missing email and irritates customers.

B. After Spam is Sent

A spam blocker is a program that blocks the spam mails entering the inbox. One method is to use a spam database, which involves gathering feedback from the user community, who reports a mail as spam when they receive it. A triggering algorithm identifies a mail as spam, when the number of reports for a particular message exceeds a given threshold. Spam blockers use this information to block the offending message from further users. Another technology is the use of spam firewall. Firewall is a system designed to prevent unauthorized access to or from a private network. Spam firewalls are installed by companies to identify and prevent spam from entering their networks. The firewall solution can be either software based or hardware based.

A new and simple method has been proposed recently is the Challenge Response Spam Filtering technique. The idea behind this method is that the spammers normally use an automated process to send email to millions of people each day, which are not monitored manually. When using this system, each email address must be authorized before delivering an email to the receiver. The receiver can either authorize these email addresses manually, or can challenge the sender to identify themselves. Until and unless the sender answers this challenge manually, the mail is considered as spam and is filtered from the receiver's mailbox and further future mails are automatically blocked.

C. After Spam is in Mailbox

The third type of anti-spam technique is the most frequently used anti-spam solution. If the spam has already reached the mailbox, then a spam filter can be installed. A spam filter is a web based, server based program installed locally, to prevent spam email from being downloaded to PC. The spam fighting program will examine the incoming email and match it against a set of pre-defined rules. If the email does not match those rules then it is either deleted or quarantined for review. This is the most popular solution for spam mails. Another solution is to use a heuristic approach to filter spam mails. Heuristic filtering works by subjecting email messages through thousands of pre-defined rules against the message envelope, header and content. Each rule assigns a numerical score to the probability of the message being spam. The spam score is then measured against the user's desired level of spam sensitivity (low, medium or high sensitivity). Based on the spam score and sensitivity threshold, the messages are organized into spam, not spam, and unsure folders.

Bayesian filtering is a recent development employed by spam blocker software and it appears to be very effective for detecting and removing spam at the personal level. Bayesian spam filters are considered intelligent, as they are capable of comparing two sets of information and acting on a result. This is a direct contrast to the vast majority of other spam filters which use pre-built rules to decide which emails are spam and which are ham. Bayesian spam filters can take one group of legitimate email and another group of spam and compare the values and data of each. Bayesian filters look for obvious repeating patterns to form an "opinion" on something. In spam filter terms that "opinion" becomes a rule which identifies spam. The main advantage here is that it is capable of learning, which can be exploited for successful spam blocking.

D. Legal Solution

A legal way to stop spam mails is brought by the Government and is called CAN SPAM Act. The CAN SPAM Act stands for Controlling the Assault of Non-Solicited Pornography and Marketing. The CAN SPAM Act 2003 was passed by the senate on November 25, 2003, which effect on January 1, 2004. The Act is to control the amount of unsolicited pornography and mass marketing that enters into the public's inboxes. To report spam, spam bureaus have been set up where the receiver can register the offenders or one can directly contact the US Federal Trade Commission to report the offensive spam. The disadvantage of this act is that it can regulate spam mails only within United States, whereas majority of the spam arise from Soviet Union and China.

Another effective commercial solution is Ciphersend, which combines encryption schemes with emails to prevent mailbox from being spammed. The Ciphersend uses 2048-bit encryption, which is much more than online banking services, which uses a 128-bit encryption or 256-bit at best.

IV. Existing Techniques

Currently, there are various forms of spam filtering techniques available. This section presents some of these works.

A. General Spam Characteristics

Antispam developers while designing filters always take the general characteristics of a spam mail into consideration. More than 99% of spam falls into one or more of the categories given below.

(i) to advertise some goods, services, or ideas

(ii) to cheat users out of their private information and to deliver malicious software

(iii) to cause a temporary crash of a mail server.

Each of the categories, in turn, is being studied by several researchers. Advertising spam mails promote different kinds of products or services, however, careful scrutiny has shown that spammers change the percentage of advertisements dedicated to each category of products or services over time [27]. The local nature on the concept also drifts over time and this was studied by [11]. Phishing activity of spammers was studied by [12], while malicious spam content characteristics were reported by [33]. Spam attacks that upset the work of a mail server was studied and reported by [35]. Characteristics of spam traffic are different from those of legitimate mail traffic in particular legitimate mail is concentrated on diurnal periods, while spam arrival rate is stable over time. This behaviour of spam mail was reported by [19]. In the same period, spammers harvesting activities, which can be used to

recognize and identify spammers was reported by [38]. A very important fact is that spammers are reactive, namely they actively oppose every successful anti-spam effort [16], so that performance of a new method usually decreases after its deployment. Pu and Webb [39] analyze the evolution of spamming techniques. They showed that spam constructing methods become extinct if filters are effective to cope with them or if other successful efforts are taken against them. A study of the network-level behavior of spammers by [40] showed that the majority of spam comes from a few concentrated parts of IP address space. Moreover, they also found that only a small subset of sophisticated spammers uses temporary route announcements in order to remain untraceable.

B. Email Transmission Protocol

One of the proposed ways of stopping spam is to enhance or even substitute the existing standards of email transmission by new, spam-proof variants. The main drawback of the commonly used Simple Mail Transfer Protocol (SMTP) is that it provides no reliable mechanism of checking the identity of the message source. Overcoming this disadvantage, namely providing better ways of sender identification, is the common goal of Sender Policy Framework (SPF, formerly interpreted as Sender Permitted From) [48], Designated Mailers Protocol (DMP) [17], Trusted Email Open Standard (TEOS) [43], and SenderID [45]. A comparison and discussion of these kinds of proposals are given by [31].

According to [22], almost 40% of legitimate email is today SenderID-compliant. The principle of its work resulted in the following: the owner of a domain publishes the list of authorized outbound mail servers, thus allowing recipients to check whether a message which pretends to come from this domain really originates from there. A discussion of the problem of fake IP addresses in email messages and ways of overcoming it by changes in standards is given by [20].

Amendment of the existing protocols that (i) represents a minor obstacle for sending few emails and (ii) a major one for sending great number of messages was extensively studied by [15]. Another proposal [44] was to establish a small payment for sending an email message, neglible for a common user, but big enough to prevent a spammer to broadcast millions of messages. An interesting version of this approach is Zmail protocol [28]. In Zmail, a small fee is paid by a sender to the receiver. Thus, a common user who sends and receives messages gets neither damage nor profit from using email, while spamming becomes a costly operation.

Another approach is to use simple tests that allow the system to distinguish human senders from robots [7], for example to ask the user to answer a moderately easy question before sending the message. One disadvantage of this approach is that such protection is annoying to human senders. Duan et al. [14] propose to use differentiated email delivery architecture to handle messages from different classes of senders in different ways. For example, some messages are kept on the sender's mail server until the receiver asks to transmit them to him.

C. Local Changes in Transmissiion

Some solutions do not require global protocol changes but propose to manage email in a different way locally. Li et al. [32] and [42] propose slowing down the operations with messages that are likely to be spam. A similar idea is discussed in the technical report by [49], who propose to use the past behaviour of senders for fast prediction of message category. The spam mails are then maintained in a lower priority queue, while the ham mails in a higher priority queue. In this way, the delivery of legitimate mail is guaranteed, but it becomes hard to broadcast many spam messages at once.

When a spammer falsifies the sender identity in the messages, the server corresponding to the falsified address receives a great number of error mails. This problem was solved in [50] by using a separate mail transfer agent for the error messages. Goodman and Rounthwaite [21] point to the possibility of controlling not only ingoing, but also outgoing spam, stopping it on the level of email service provider used by a spammer.

D. Language- Based Filters

Another group of methods use the fact that the message body is a text in a natural language. These methods can be applied to message headers or whole messages. The main motivation for their application on spam filtering relies on the fact that they are effective in natural language text classification. In fact, the same motivation can also be applied to the methods based on compression models. Examples of such models include dynamic Markov compression and prediction by partial matching. They were successfully used with the data extracted from both bodies and headers of the messages [5].

Chi by degrees of freedom method, previously used for document authorship identification, is proposed for spam filtering by [36]. Messages are represented in terms of character or word Ngrams. The idea of the method is to compare the new message to the spam and legitimate messages in the training data using the chi-by-degrees-of freedom (CDF) test. The CDF is calculated by dividing the value of the $\chi 2$ test by the number of degrees of freedom.

Smoothed N-gram language models, proposed by [34], used smoothed higher order N-gram models. N-gram language models are based on the assumption that the existence of a certain word at a certain position in a sequence depends only of the previous N-1 words.

E. Non-Content Features

The methods based on structured analysis of the header and of meta-level features, such as number of attachments, use specific technical aspects of email and so they are specific to spam filtering. Leiba et al. [30] proposed a method called analyzing SMTP path to detect spam. The filtering method was based on analyzing IP addresses in the reverse-path and ascribing reputation to them according to amount of spam and legitimate mail delivered through them. Both this and the subsequent method can be viewed as development of the idea of blacklisting and whitelisting.

Analyzing the user's social network is another algorithm proposed by [4]. They analyzed the 'From', 'To', 'Cc' and 'Bcc' fields of the message headers in order to build a graph of social relations of the user, and then uses this graph in order to classify new messages. The idea of extracting the user's social network from his mailbox was further developed by [8] and [18].

Behavior-based filtering rests on extracting knowledge about the behavior behind a given message or group of messages from their non-content features. Later detect spam by comparing it to the predefined or extracted knowledge about the typical behaviors of malicious and normal users. Examples are the works of [52] and [25]. Yeh et al. [52] use well-known behaviors of spammers, such as using incorrect dates. Hershkop [25] proposes a number of behavior models based on non-content features, which can be used to detect spam and viruses as anomalies in the email flow. Examples of such models include recipient frequency and histograms of user's past activity.

F. Content Based Classification

One popular practice when creating spam pages is "Keyword Stuffing", where the keywords within a web page (excluding markup) is analyzed to detect spam mails. Excessive appearance of keywords in the title of a page is a clear indication of spam. Content-based Naive Bayes (PGRAM) is another technique for the classification of Image spam. Graham [23] found out that the task of spam detection has floated the idea of a partial Naïve Bayes approach, biased towards low false positive rates. It also uses word tokens, but filters out predefined common tokens.

The content and the header of the incoming email are mostly analyzed by the available anti-spam techniques. They try to infer something about the kind of the material contained in the message by looking for specific pattern typical of a spam message. For these reasons, these filters are known as "content based." There are many anti-spam techniques available that falls under this category.

Blacklist and White list filters check whether the incoming message is from a known and trusted email address. Rule based filters correlate a score to every incoming email calculated according to a set of rules based on typical features of spam messages (fake SMTP components, Keywords, HTML formatting, etc) [9]. In case the score exceeds the given threshold value it is recognized to be a spam message. Major problem in this method is that, since its semantics are not well defined, it is difficult to aggregate rules and ascertains a threshold that limits the number of false positives. Spamassassin results from the successful implementation of the above-mentioned technique.

G. Hybrid Filters

Studies were also conducted, which analyze the possibility of combining different algorithms for spam filtering. Most of the research implements this approach if they use unrelated features to produce a solution [30, 53]. Existing technologies and algorithms focus on individual parameters of the malicious content. However, efficiency of the filtering techniques gets significantly reduced when special forging techniques are used and the shortcomings of individual algorithms are exploited. The hybrid technique can be implemented by using various models, considering available resources with the server. He et al. [24] proposed a framework which combines white/black listing and challenge-response methods. Bhuleskar et al. [2], after identifying the advantages and disadvantages of various filters, combines the advantages of the various filtering techniques and proposes a hybrid filter.

In an enterprise environment, the commercial hybrid system Brightmail [6] enjoys a good reputation. Companies rely on Brightmail, as it offers a good performance and the necessary professional support to keep the system up to date. Since Brightmail does not offer a home user solution, the freeware Spampal [47] is better suited for individual users. There are several different, free filters available on the internet which can be included in Spampal, and the user has a free choice which of them to use. Unfortunately, Spampal is only available for Microsoft Windows operating systems. Linux users can work with [46], which is also evolving into a full featured hybrid tool.

Hybrid solutions need to be carefully designed as the combination might increase time complexity while increasing security and accuracy.

V. EVALUATION METHODS

The great number and variety of spam filtering methods results in the need for evaluation and comparison of them. The usual way of testing a filter is applying it to a corpus of previously gathered mail messages sorted into spam and legitimate mail. The most simple measure used to express the results of such testing is filtering accuracy, namely percentage of messages classified correctly [29], which has the disadvantage of making no difference between false positives and false negatives. More informative measures are spam/ham recall and spam/ham precision. In Table 2 $nL \rightarrow L$ and $nS \rightarrow S$ are the number of ham and spam messages classified correctly. Similarly, $nL \rightarrow S$ and $nS \rightarrow L$ are the numbers of ham and spam messages misclassified and λ is the relative cost of the two type of errors.

VI. CONCLUSION

This paper provided a brief introduction to the concept of spam emails with emphasis on image-spam emails along with a review study, that discussed various solution provided for this problem. As spammers have innumerable techniques for creating a spam image, the research for a perfect spam filter is always fertile. Several works have been proposed and almost all of these methods have the common objectives of high processing speed and high accuracy, to make it applicable in time critical environment like the Internet. Even though legal solutions have been adopted, it is still in its infantry stage and is not of much use for countries other than US. Image spam filtering technique still needs for more research to reach 100% accuracy. Future work includes analysis and comparison of these some techniques reviewed in terms of computation and time complexity along with accuracy.

TABLE I. MEASURES OF FILTERING PERFORMANCE

Measure	Formula
Accuracy	$\frac{n_{L\to L}+n_{S\to S}}{n_{S\to S}+n_{S\to L}+n_{L\to S}+n_{L\to L}}$
Error rate	$\frac{n_{L\to S}+n_{S\to L}}{n_{S\to S}+n_{S\to L}+n_{L\to S}+n_{L\to L}}$
False positive rate	$\frac{n_{L\to S}}{n_{L\to S}+n_{L\to L}}$
Spam recall	$\frac{n_{S\to S}}{n_{S\to S}+n_{S\to L}}$
Spam precision	$\frac{n_{S\to S}}{n_{S\to S}+n_{L\to S}}$
Ham recall	$\frac{n_{L\to L}}{n_{L\to S}+n_{L\to L}}$
Ham precision	$\frac{n_{L\to L}}{n_{L\to L}+n_{S\to L}}$
Weighted accuracy	$\frac{\lambda n_{L\to L}+n_{S\to S}}{\lambda(n_{L\to L}+n_{L\to S})+n_{S\to L}+n_{S\to S}}$
Weighted error rate	$\frac{\lambda n_{L\to S}+n_{S\to L}}{\lambda(n_{L\to L}+n_{L\to S})+n_{S\to L}+n_{S\to S}}$
Total Cost Ratio	$\frac{n_{S\to L}+n_{S\to S}}{\lambda n_{L\to S}+n_{S\to L}}$
False Detection Rate (FDR)	$\frac{n_{L\to S}}{n_{L\to S}+n_{S\to S}}$
False Positive Rate (FPR)	$\frac{n_{L\to S}}{n_{L\to S}+n_{L\to L}}$
ROC	True positive rate plotted against false positive rate

REFERENCES

[1] Androutsopoulos, I., Koutsias, J., Chandrinos, K. and Spyropoulos, C., "An experimental comparison of naïve Bayesian and keyword-based anti-spam filtering with personal e-mail messages," Proceedings of the International ACM SIGIR Conference, 2000.

[2] Bhuleskar, R., Sherlekar, A. and Pandit, A., "Hybrid Spam E-mail Filtering," First International Conference on Computational Intelligence, Communication Systems and Networks, pp.302-307, 2009.

[3] Bowling, J.R., Hope, P. and Liszka, K.J., "Spam image identification using an artificial neural network," MIT SPAM Conference, pp.1-11, 2008.

[4] Boykin, P. and Roychowdhury, V., "Leveraging social networks to fight spam," Computer, vol.38, no.4, pp.61–68, 2005.

[5] Bratko, A., Cormack, G.V., Filipic, B., Lynam, T.R. and Zupan, B., "Spam filtering using statistical data compression models, Journal of Machine Learning Research, vol. 7, pp. 2673–2698, 2006.

[6] Brightmail, "Spam Percentages and Spam Categories," http://www.brightmail.com/ spamstats.html, Last Access Date : January, 2011.

[7] CAPTCHA (2005), The CAPTCHA project. http://www.captcha.net, Last Access Date : January, 2011.

[8] Chirita, P.A. Jo, D. and Nejdl, W. Mailrank, "Using ranking for spam detection," Proceedings of the 14th ACM International Conference on Information and Knowledge Management, CIKM 2005, ACM Press, Pp. 373–380, 2005.

[9] Cohen, W.W., "Learning Rules that Classify E-Mail," Papers from the AAAI Spring Symposium on Machine Learning in Information Access, AT&T Laboratories, pp. 18-25, 1996.

[10] Cumming, J.G., "The Spammer'sCompendium," http://www.jgc.org/ tsc.html, 2010.

[11] Delany, S.J., Cunningham, P., Tsymbal, A. and Coyle, L., "A case-based technique for tracking concept drift in spam filtering," Knowledge-based systems, pp. 187–195, 2004.

[12] Drake, C., Oliver, J. and Koontz, E., "Anatomy of a phishing email," Proceedings of the First Conference on Email and Anti-Spam, CEAS'2004, 2004.

[13] Dredze, M., Gevaryahu, R. and Bachrach, A.E., "Learning Fast Classifiers for Image Spam," Fourth Conference on Email and Anti-Spam (CEAS 2007) Mountain View, California, 2007.

[14] Duan, Z., Dong, Y. and Gopalan, K., "Diffmail: A differentiated message delivery architecture to control spam," Proceedings of 11th International Conference on Parallel and Distributed Systems, ICPADS 2005, Vol. 2, pp. 255–259.

[15] Dwork, C. and Naor, M., "Pricing via processing or combating junk mail," Advances in Cryptology - Crypto 92 Proceedings, Springer Verlag, pp.139-147, 1992.

[16] Fawcett, T., "in vivo" spam filtering: a challenge problem for data mining," KDD Explorations, vol. 5, no.2, pp.140–148, 2003.

[17] Fecyk, G., "Designated mailers protocol," www.panam.ca/ dmp/draft-fecyk-dmp-01.txt, Last Access Date : January, 2011.

[18] Golbeck, J. and Hendler, J., "Reputation network analysis for email filtering," Proceedings of the First Conference on Email and Anti-Spam, Mountain View, CA, USA, 2004.

[19] Gomes, L.H., Cazita, C., Almeida, J.M. Virgı, A. and Meira, W., "Characterizing a spam traffic," IMC '04: Proceedings of the 4th ACM SIGCOMM conference on Internet measurement, pages 356–369, New York, NY, USA, ACM Press. ISBN 1-58113-821-0, 2005.

[20] Goodman, J., "IP addresses in email clients," Proceedings of the First Conference on Email and Anti-Spam, CEAS'2004.

[21] Goodman, J. and Rounthwaite, R., "Stopping outgoing spam," EC'04: Proceedings of the Fifth ACM Conference on Electronic Commerce, 2004.

[22] Goodman, J., Cormack, G.V. and Heckerman, D., "Spam and the ongoing battle for the inbox," Communications of the ACM, vol.50, no.2, pp.25–33, 2007.

[23] Graham, P., "A plan for spam," http://www.paulgraham.com/spam.html, Last Access Date : January, 2011.

[24] He, P., Sun, Y., Zheng, W. and Wen, X., "Filtering short message spam of group sending using CAPTCHA," In: Workshop on knowledge discovery and data mining, pp. 558–561, 2008.

[25] Hershkop, S., "Behavior-based email analysis with application to spam detection," PhD Thesis, Columbia University, 2006.

[26] Hope, P., "Using artificial neural networks to identify image spam," a thesis presented to the graduate faculty of the University of Akron in partial fulfillment of the requirements for the Degree Master of Science, 2008.

[27] Hulten, G., Penta, A., Seshadrinathan, G. and Mishra, M., "Trends in spam products and methods," Proceedings of the First Conference on Email and Anti-Spam, CEAS'2004, pp.1-2, 2004.

[28] Kuipers, B., Liu, A., Gautam, A. and Gouda, M., "Zmail: zero-sum free market control of spam," Proceedings of the 25th IEEE International Conference on Distributed Computing Systems Workshops, ICDCS 2005, IEEE Computer Society, pp. 20–26, 2005.

[29] Lai, C.C. and Tsai, M.C., "An empirical performance comparison of machine learning methods for spam e-mail categorization," Hybrid Intelligent Systems, pp. 44-48, 2004.

[30] Leiba, B., Ossher, J., Rajan, V.T., Segal, R., and Wegman, M., "SMTP path analysis," Proceedings of Second Conference on Email and Anti-Spam, CEAS'2005.

[31] Levine, J. and Dekok, A., "Lightweight MTA authentication protocol (LMAP) discussion and comparison," www.taugh.com/draftirtf- asrg-lmap-discussion-01.txt, Last Access Date : January, 2011.

[32] Li, K., Pu, C. and Ahamad, M., "Resisting spam delivery by TCP damping," Proceedings of the First Conference on Email and Anti-Spam, CEAS'2004.

[33] Lugaresi, N., "European union vs. spam: A legal response," Proceedings of the First Conference on Email and Anti-Spam, CEAS'2004.

[34] Medlock, B., "An adaptive approach to spam filtering on a new corpus," Proceedings of the Third Conference on Email and Anti-Spam, CEAS'2006.

[35] Nagamalai, D., Dhinakaran, C. and Lee, J.K., "Multi layer approach to defend DDoS attacks caused by spam," MUE'07, International Conference on Multimedia and Ubiquitous Engineering, pp. 97–102, 2007.

[36] O'Brien, C. and Vogel, C., "Spam filters: bayes vs. chi-squared, letters vs. words," Proceedings of the 1st international symposium on Information and communication technologies, ISICT '03, Trinity College Dublin, Ireland pp. 291–296, 2003.

[37] Pew Internet and American Life Project data, "Trend Data," http://www.pewinternet.org/Static-Pages/Trend-Data/Online-Activites-Total.aspx, Last Access Date : January, 2011.

[38] Prince, M., Dahl, B., Holloway, L., Keller, A. and Langheinrich, E., "Understanding how spammers steal your e-mail address: An analysis of the first six months of data from project honey pot," Proceedings of Second Conference on Email and Anti-Spam, CEAS'2005, Mountain View, CA, USA.

[39] Pu, C. and Webb, S., "Observed trends in spam construction techniques: A case study of spam evolution," Proceedings of Third Conference on Email and Anti-Spam, CEAS'2006.

[40] Ramachandran, A. and Feamster, N., "Understanding the network-level behavior of spammers," SIGCOMM'06, Proceedings of the 2006 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications, 2006.

[41] Riedel, J. and Brown, Z., "The Evolution of Spam and SpamAssassin," A Major Qualifying Project Report submitted to the Faculty of the Worcester Polytechnic Institute in partial fulfillment of the requirements for the Degree of Bachelor of Science, 2004.

[42] Saito, T., "Anti-spam system: Another way of preventing Spam," Proceedings of the 16th International Workshop on Database and Expert Systems Applications, DEXA 2005, pp. 57–61, 2005.

[43] Schiavone, V., Brussin, D., Koenig, J., Cobb,S. and Everett-Church, R., "Trusted e-mail open standard: A comprehensive policy and technology proposal for email reform," http://www.cobb.com/spam/teos, 2003, Last Access Date : January, 2011.

[44] Seltzer, L., "Should senders pay for the mess we call e-mail? eWeek," http://www.eweek.com/ article2/0,4149,1273186,00.asp, 2003, Last Access Date : January, 2011.

[45] SenderID, "Sender ID technology: Information for IT professionals," www.microsoft.com/mscorp/safety/technologies/senderid/technology.mspx, 2004, Last Access Date : January, 2011.

[46] Spamassassin, http://www.spamassassin.org, 2004, Last Access Date : January, 2011

[47] Spampal, http://www.spampal.org, 2004, Last Access Date : January, 2011

[48] SPF FAQ, http://openspf.org/faq.html, 2010, Last Access Date : January, 2011.

[49] Twining, R.D., Williamson, M.M., Mowbray, M. and Rahmouni, M., Email prioritization: reducing delays on legitimate mail caused by junk mail, Technical Report HPL-2004-5R1, HP Labs, 2004.

[50] Yamai, N., Okayama, K., Miyashita, T., Maruyama, S. and Nakamura, M., "A protection method against massive error mails caused by sender spoofed spam mails," Proceedings of the 2005 Symposium on Applications and the Internet, SAINT 2005, pp. 384–390, 2005.

[51] Yamasaki, T.,Email Statistics Report, 2010-2014, "*Key Statistics for Email, Instant Messaging, Social Networking and Wireless Email,"* The Radicati Group, Inc., http://www.radicati.com, 2005, Last Access Date : January, 2011.

[52] Yeh, C.Y., Wu, C.H. and Doong, S.H., "Effective spam classification based on meta-heuristics," In Proceedings of IEEE International Conference on Systems, Man and Cybernetics, SMC 2005, vol. 4, pp.3872–3877, 2005.

[53] Zhang, L., Zhu, J. and Yao, T., "An Evaluation of Statistical Spam Filtering Techniques," ACM Transactions on Asian Language Information Processing, vol.3, no.4, pp.243-269, 2004.