ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

A REVIEW: TYPE SPECIFICATION BASED VIDEO SPAM DETECTION

Pooja Kamboj*, Er. Chandna Jain
M.Tech, CSE, JCDM College of Engineering, Sirsa, India.
Asst Professor, CSE, JCDM College of Engineering, Sirsa, India.

ABSTRACT

Video sharing websites are most popular services for share video among the number of users. These websites also connect with different kind of users known as social networking Web Services. But in these services, there are different kinds of pollution related to the video such as uploading of malicious, copyright violated and spam video or content. The users upload the video for the particular category and viewers/responders response the video by commenting, share video related to the uploaded video but malicious users does not share related video. The users share the unrelated information, abusive or pornographic, commercial video or it can be automatically scripts. These videos are the responsive videos. This research work presents a method for detection of such kind of responses. The first phase of detection is to divide the problem in different scenarios and define the keywords in database which can be related to commercial and pornographic. The sample dataset will contain all the information and video for analysis of the videos and categorized as per content type. The different kind of techniques will identify the video and with some features such as presence of certain terms in the title or description, Likes, elapsed time, uploaded time, etc. The different kind of videos data collection will be considered for analysis the algorithm and corresponding result will be generated. The research will be demonstrated using MATLAB TOOL which will contains the sample videos for Analyze the spam detection, porn video and commercial videos. The website will also save the keywords and these words will be update frequently and remove outdated words for improved detection of videos.

.

KEYWORDS: Elapsed time, Token, Description.

INTRODUCTION

The web is growing with the emerging of new technologies and consist the different kinds of services which contains the Photo Sharing, Social networking websites, Email Services, Video Sharing and Downloading, Sound Transmission and Live chat, promotional web services, Payment Services, Net Banking and many other Service providers are in queue. Social networking web Services create a scenario in which people can socialize and communicate throughout the world, examples of such social networking sites are Twitter, Facebook and MySpace. Users of these sites are able to add a wide variety of information to pages, to pursue common interests, and to connect with others. There are also business related web sites such as LinkedIn and these kinds of services used for business connections. For videos service, the YouTube is most popular web service by Google.

There are number of users who are interested in games and videos, and such kind of websites also has the section for video and games. But the industries related to their business and having great revenue by taking advantage of pornography and videos over the World Wide Web. For the revenue purpose, the industries are posting unrelated videos with respect to the related videos.

The users are searching something on internet but the searched content is not related to the user's requirement. For example, User is searching for the game of child but in another section, user is getting the porn video or such kind of advertisement which comes under the area of Spam. Being such a popular video sharing site, it become a platform for spammers and promoters to post unrelated and irrelevant content either as video response or as related video to the most popular videos either to gain popularity or to promote their sites or products. The term Spam can be defined, that is some inappropriate message posted over the internet web services, especially to large number of users with the intention of either getting publicity or to spread viruses, malwares.

Spam in domains such as emails, web-pages, blogs, social networking websites, online discussion forums, wikis and video sharing websites is prevalent and naturally has several negative impacts such as undesirable consumption of computing resources, lowering the reputation or value of the targeted legitimate web application, impacting search engine rankings, overwhelming moderators and administrators, and obstructs and misleads genuine usage of legitimate users and community.

The study shows that the interested user of particular video is getting the irrelevant video which is actually posted for the purpose of attraction towards the video which can be porn, commercial video and helpful for the company's profit. Video responses are the videos which are in response to the searched video content and related video which are matched with the searched content. The video responses can be detected as spam by analyze the title, description, uploading time, duration, number of Likes, etc in video responses and also in the related videos. The number of detection approached will be used for find the spam video which will analyze the video by counting of porn or commercial words and calculate its percentage. The complete approaches are explained in this paper described later.

Fig. 1 Example of Spam on Web

Recently, online social networking services such as Facebook, Wikipedia and YouTube are experiencing a dramatic growth in terms of popularity. In particular, video content is becoming a predominant part of users' daily lives on the Web. By allowing users to generate and distribute their own multimedia content to large audiences, the Web is being transformed into a major channel for the delivery of multimedia. Video pervades the Internet and supports new types of interaction among users, including political debates, video chats, Video Responses, comments, video mail, and video blogs. A number of Web services are offering video-based functions as alternative to text-based ones, such as video reviews for products, video ads and video responses. In particular, the video response feature allows users to converse through video, by creating a video sequence that begins with an opening video and then followed with video responses from fans and detractors.

By allowing users to publicize and share their independently generated content, social video sharing systems may become susceptible to different types of malicious and opportunistic user actions, such as self-promotion, video aliasing and video spamming. We define a video response and related video spam as a video posted as a response to an opening video, but whose content is completely unrelated to the opening video. Video spammers are motivated to spam in order to promote specific content, advertise to generate sales, disseminate pornography or compromise the system reputation. Spamming has been observed in several different contexts, including email, Web search engines and blogs. A numbers of spam detection techniques exploit characteristics present in the Video (e.g., Title, Description). Moreover, users of such systems can quickly learn to identify some Video spams e.g., by hyperlink, likes, duration etc.

Detection approach

The detection approach consists of first retrieving video's detail marked with binary variable hasSpamHint flag for a given video and this flag can true or false. The hasSpamHint will be calculated by different scenarios. This hint calculated by parameters such as words percentage in Description, title and time difference. If the parameters exceed by threshold, then this flag will be activated, will be described in the detection techniques. The next step consists of computing the values of variables indicating the spam intention of user (as spammer). We define different indicators and describe our intuition behind the proposed indicators. The value of the following indicators is then used to score a give user as Botnet, Commercial and Pornographic Spammer.

ATDVU

Average Time Difference between Video Upload (ATDVU): We extract all the recent video uploading time; the number of videos uploaded that can retrieved and computes the time differences between all the video. We compute the average time difference and record the value. We hypothesize that a low value of ATDC signals spam. Our conjuncture is based on the observation that spammers often employ automated scripts and can be concluded as botnet videos in which the time difference between subsequent video uploaded is so low that it is not manually feasible.

PWAHF

Percentage of Words in Attributes with hasSpamHint Flag (PWAHF): Firstly, We will count the porn and commercial words and compute the percentage. If the percentage of the calculated words is exceeding the threshold, it means the video is count as spam. We hypothesize that a significant percentage by a user marked as hasSpamHint can be used as a signal for classifying the user as spammer. We notice several users who are spammers (validated based on manual inspection) exhibit a high PWAHF value.

SUOWD

Store and Update outdated Words Dictionary Update (SUOWD): In this, we will firstly store the porn words and commercial words as well. The stored words will be compared with the words in title, description and then percentage computation will be analyzed. On the frequent search on Internet, the Words will be updated because the old words will not be used in video response and will not be able to identify spam. So the updating in database will help to identify the latest spam video and categorize accordingly that is porn or commercial spam.

STV

Settlement Threshold variable (STV): The threshold value will be initialized. This variable will be varying according to the words count condition. If the length of the title, description is short, then this variable will be high value otherwise it will low. This threshold will vary as per the condition and it can be any value.

Types of Spam

There are number of spam types which can be used for commercial purpose and business related activities. These are classified as:

Email

Email spam, also known as unsolicited bulk Email, junk mail, or unsolicited commercial email, is the practice of sending unwanted email messages, frequently with commercial content, in large quantities to a random set of recipients. Email Spam problem issue growing exponentially. The option is also available to make Email spam illegal which has been successful up to some level. The email spam are transmitting at regular interval via a networks which are interrelated network of networks contains virus and worms which have been affected the office and personal computers. The spammer's use for access the computers and it has been used for the illegal activities. There are different kinds of authors which are working together for gather the private information and use it. There are different kind of industries who have resources only for gather and collect the email addresses and sold the information which can be successful by database at back end server.

Mobile phone

Mobile phone spam is directed at the text messaging service of a mobile phone. This can be especially irritating to customers not only for the inconvenience but also because of the fee they may be charged per text message received

in some markets. To comply with CAN-SPAM regulations, now SMS messages have to have the options of HELP and STOP, the latter to end communication with the advertising spam altogether.

Instant messaging

Instant messaging spam makes use of instant messaging systems. Although less ubiquitous than its e-mail counterpart, 500 million spam IMs were sent in 2003, twice the level of 2002. The instant messaging tends to not be blocked by firewalls; it is an especially useful channel for spammers. This is very common on many instant messaging systems such as Skype.

Newsgroup and forum

Newsgroup spam is a type of spam where the targets are Usenet newsgroups. Spamming of Usenet newsgroups actually pre-dates e-mail spam. Usenet convention defines spamming as excessive multiple posting, that is, the repeated posting of a message or substantially similar messages.

Forum spam is the creating of messages that are advertisements on Internet forums. It is generally done by automated spam bots. Most forum spam consists of links to external sites, with the dual goals of increasing search engine visibility in highly competitive areas such as weight loss, pharmaceuticals, gambling, pornography, real estate or loans, and generating more traffic for these commercial websites. Some of these links contain code to track the spam bots identity; if a sale goes through, the spammer behind the spambot works on commission.

Social networking spam

Facebook and Twitter are not immune to messages containing spam links. Most insidiously, spammers hack into accounts and send false links under the guise of a user's trusted contacts such as friends and family. In Twitter, spammers gain credibility by following verified accounts; when that account owner follows the spammer back, it legitimizes the spammer and allows him or her to proliferate.

Social spam

Spreading beyond the centrally managed social networking platforms, user-generated content increasingly appears on business, government, and nonprofit websites worldwide. Fake accounts and comments planted by computers programmed to issue social spam can infiltrate these websites. Well-meaning and malicious human users can break websites' policies by submitting profanity, insults, hate speech, and violent messages.

Online game messaging

Many online games allow players to contact each other via player-to-player messaging, chat rooms, or public discussion areas. What qualifies as spam varies from game to game, but usually this term applies to all forms of message flooding, violating the terms of service contract for the website. This is particularly common in MMORPGs where the spammers are trying to sell game-related “items” for real-world money, chiefly among them being in-game currency.

Spam targeting search engines (spamdexing)

Spamdexing refers to a practice on the World Wide Web of modifying HTML pages to increase the chances of them being placed high on search engine relevancy lists. These sites use “black hat search engine optimization (SEO) techniques” to deliberately manipulate their rank in search engines. Many modern search engines modified their search algorithms to try to exclude web pages utilizing spamdexing tactics. For example, the search bots will detect repeated keywords as spamming by using a grammar analysis. If a website owner is found to have spammed the webpage to falsely increase its page rank, the website may be penalized by search engines.

Blog, wiki, and guestbook

Blog spam is spamming on weblogs. This type of spam took advantage of the open nature of comments in the blogging software Movable Type by repeatedly placing comments to various blog posts that provided nothing more than a link to the spammer's commercial web site. Similar attacks are often performed against wikis and guestbook’s, both of which accept user contributions. Another possible form of spam in blogs is the spamming of a certain tag on websites such as Tumbler.

User Test Collection

In order to evaluate our proposed approach to detect video spammers and promoters in online video social networking systems, we need a test collection of users, pre-classified into the target categories, namely, spammers, promoters and, in lack of a better term, legitimate users. However, to the best of our knowledge, no such collection is publicly available for any video sharing system, thus requiring us to build one.

Before presenting the steps taken to build our user test collection, we introduce some notations and definitions. We say a YouTube video is a responded video or a video topic if it has at least one video response. Similarly, we say a YouTube user is a responsive user if she has posted at least one video response, whereas a responded user is someone who posted at least one responded video.

Moreover, we define as spammer a user who posts at least one video response that is considered unrelated to the responded video (i.e., a spam). Examples of video spams are:
1. An advertisement of a product or website completely unrelated to the subject of the responded video,
2. Pornographic content posted as response to a cartoon video. A promoter is defined as a user who posts a large number of video responses to a responded video, aiming at promoting this video topic
A user that is neither a spammer nor a promoter is considered legitimate.

LITERATURE REVIEW

[1] Yuan Niu, Yi-Min Wang explains the comprehensive study with different consideration of forum Spamming. The author has evaluated the impact of forum spamming on search quality and conducted a Comprehensive study from three perspectives: that of the search user, the spammer, and the forum hosting site. Author examines spam blogs and spam comments in both legitimate and honey forums. The study shows that forum spamming is a widespread problem. Spammed forums, powered by the most popular software, show up in the top 20 search results for all the 189 popular keywords. On two blog sites, more than half (75% and 54% respectively) of the blogs are spams, and even on a major and reputably well maintained blog site, 8.1% of the blogs are spam1. The observation confirms that spammers target abandoned pages and that most comment spam is meant to increase page rank rather than generate immediate traffic. Authors propose context based analyses, consisting of redirection and cloaking analysis, to detect spam automatically and to overcome shortcomings of content-based analyses. This paper shows that these analyses are very effective in identifying spam pages.

[2] Alan Mislove Massimiliano Marcon Krishna P. Gummadi assimilated the knowledge about Online social networking sites like Orkut, YouTube, and Flickr which are among the most popular sites on the Internet. Users of these sites form a social network, which provides a powerful means of sharing, organizing, and finding content and contacts. The popularity of these sites provides an opportunity to study the characteristics of online social network graphs at large scale. Understanding these graphs is important, both to improve current systems and to design new applications of online social networks. This paper presents a large-scale measurement study and analysis of the structure of multiple online social networks. They examine data gathered from four popular online social networks: Flickr, YouTube, LiveJournal, and Orkut. They crawled the publicly accessible user links on each site, obtaining a large portion of each social network's graph. Their data set contains over 11.3 million users and 328 million links. They believe that this is the first study to examine multiple online social networks at scale. Their results confirm the power-law, small-world, and scalefree properties of online social networks. They observe that the indegree of user nodes tends to match the outdegree; that the networks contain a densely connected core of high-degree nodes; and that this core links small groups of strongly clustered, low-degree nodes at the fringes of the network. Finally, we discuss the implications of these structural properties for the design of social network based systems.

Fabricio Benevenuto Fernando Duarte [9] seeks understanding the user behavior in a social network created essentially by video interactions. We present a characterization of a social network created by the video interactions among users on YouTube, a popular social networking video sharing system. Our results uncover typical user behavioral patterns as well as show evidences of anti-social behavior such as self promotion and other types of content pollution.

[3] Archana Bhattarai, Vasile Rus, and Dipankar Dasgupta explained that the Spams are no longer limited to emails and WebPages. The increasing penetration of spam in the form of comments in blogs and social networks has started

becoming a nuisance and potential threat. In this work, we explore the challenges posed by this type of spam in the blogosphere with substantial generalization regarding other social media. Thus, we investigate the characteristics of comment spam in blogs based on their content. The framework uses some of the previously explored methods developed to effectively extract the features of the blog spam and also introduces a novel method of active learning from the raw data without requiring training instances. This makes the approach more flexible and realistic for such applications. We also incorporate the concept of cotraining for supervised learning to get accurate results. The preliminary evaluation of the proposed framework shows promising results.

[4] FabrIcio Benevenuto, Tiago Rodrigues explained the article characterizes video-based interactions that emerge from YouTube's video response feature, which allows users to discuss themes and to provide reviews for products or places using much richer media than text. Based on crawled data covering a representative subset of videos and users, we present a characterization from two perspectives: the video response view and the interaction network view. In addition to providing valuable statistical models for various characteristics, our study uncovers typical user behavioral patterns in video-based environments and shows evidence of opportunistic behavior.

[5] Haifeng Yu, Michael Kaminsky, Phillip B. Gibbons, Member explained Peer-to-peer and other decentralized, distributed systems are known to be particularly vulnerable to sybil attacks. In a sybil attack, a malicious user obtains multiple fake identities and pretends to be multiple, distinct nodes in the system. By control- ling a large fraction of the nodes in the system, the malicious user is able to "out vote" the honest users in collaborative tasks such as Byzantinefailure defenses. This paper presents SybilGuard,a novel protocol for limiting the corruptive influences of sybil attacks. Author explained the protocol is based on the "social network" among user identities, where an edge between two identities indicates a human-established trust relationship. Malicious users can create many identities but few trust relationships. Thus, there is a disproportionately small "cut" in the graph between the sybil nodes and the honest nodes. SybilGuard exploits this property to bound the number of identities a malicious user can create. They show the effectiveness of SybilGuard both analytically and experimentally. This paper presented SybilGuard, a novel decentralized pro- tocol for limiting the corruptive influences of sybil attacks, by bounding both the number and size of sybil groups. SybilGuard relies on properties of the users' underlying social network, namely that (i) the honest region of the network is fast mixing, and (ii) malicious users may create many nodes but relatively few attack edges. In all our simulation experiments with one million nodes, SybilGuard ensured that (i) the number and size of sybil groups are properly bounded for 99.8% of the honest users, and (ii) an honest node can accept, and be accepted by, 99.8% of all other honest nodes.

[6] Yinglian Xie, Fang Yu,Kannan Achan has been explained the Botnets and spamming for detection of the botnet-based spam emails. Author has been developed the spam signature generation framework called AutoRE to detect botnet-based spam emails and botnet membership. AutoRE does not require pre-classified training data or white lists and outputs high quality regular expression signatures that can detect botnet spam with a low false positive rate. Using a three-month sample of emails from Hotmail, AutoRE successfully identified 7,721 botnet-based spam campaigns together with 340,050 unique botnet host IP addresses and these observations are useful information in the design of botnet detection schemes.

[7] Mark David Spadafora has introduces the methodologies presently used for the identification of spam email campaigns and the way in which these identified campaigns are used to ascertain specific strategies used in spam delivery. To understand how a spammer operates, it is not enough to simply look at the sum of all of spam messages, to establish a wider understanding, spam messages must be first grouped into campaigns and these campaigns studied as a subset to expose inherent characteristics among spam orchestration operations. From the discussion presented in this paper, the approaches taken, Spamcraft and CCSS, have been compared and contrasted against each other to explore the advantages and disadvantages of their methods for the identification of spamming strategies.

Three points of comparison between the papers were used to bridge the divide between the approaches, Data Collection, Campaign Identification and Strategy Identification. From looking at these phases, it is seen that there are several concerns pertaining to the way in which data is collected. There are ethical considerations that have been ignored, as well as the way in which their data collection procedures may be detected. It has been identified that neither of the methodologies taken provide a picture that encompasses the overall state of spamming strategies, with CCSS

focusing on the Network Level side of spam distribution and Spamcraft focusing on spam message composition. Both of these add to different aspects on the war on spam, Spamcraft helping to understand End-to-End distribution, and CCSS, discovering network level abuse. For a view that truly encompasses spamming strategies, a combination of the two approaches will ultimately be required.

PROPOSED METHODOLOGY

1. Problem Statement

In Video Sharing Websites, there are number of videos and of different types such as child Videos, Pornography, Commercial Videos, Fun Video, etc. These websites provides the user interface for the clients to search the required video but the problem is of video response. When the user searches the videos, it also shows the related videos as well as response videos. The related videos are the same as searched videos. But the response videos are posted by the user as reply or comment of searched video. The users respond to the particular video and this response may or may not be related to the video which will be count as Spam. The spam detection of response videos is major issue. User responds the videos for increase the attraction to particular content or for the commercial purposes.

a. Study of Commercial and Porn Words Dictionary.
b. Study of identification Parameters for porn and Commercial Videos.
c. Detect Spam for the Searched Videos.
d. Analyze the Porn Video Response.
e. Analyze the Commercial Video Reponses.

2. Methodology

a. Study of Existing Spam Detection Techniques.
b. Identify the benefits of the Existing Methods.
c. Research of new Spam Detection Technique.
d. Initialize the words Dictionary includes Porn and Commercial.
e. Analyze Title, Description, Uploaded Video time, Timestamp, etc. of response video with searched video and compare words with database dictionary.
f. Identify the Commercial Spam and Porn Spam based on Words Percent.
g. The result will be generated and display the spam videos.

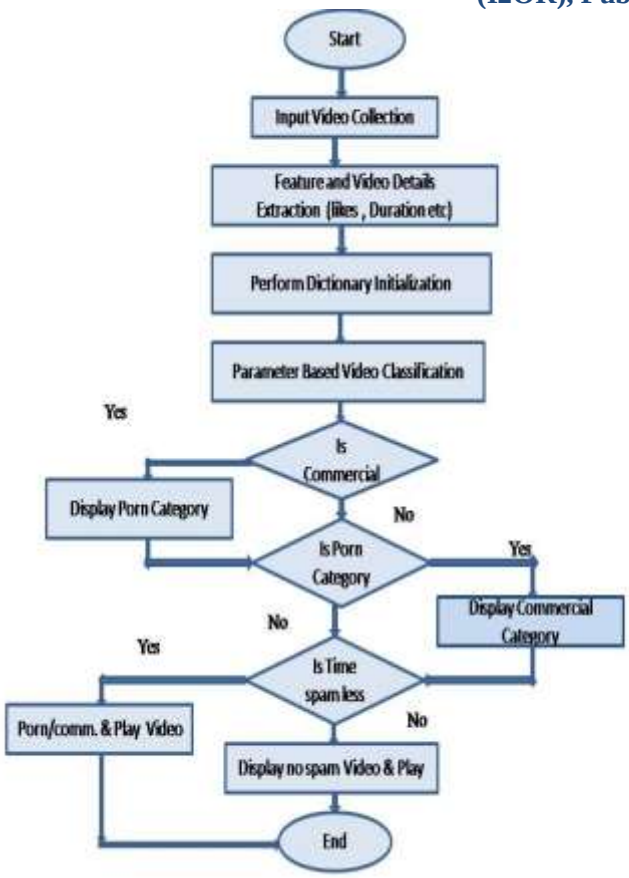

Fig. 2 Proposed Flow Chart

Objective

There is presence of spam on the most popular video sharing site i.e. YouTube and has several disadvantages. It requires researcher's attention to solve the video response spam problem on YouTube. The research aim of the work presented in this report is the following:

a. Identify the Spam on Video Sharing Websites.
b. Recognize the Porn, Commercial Videos.
c. Design web portal with Proposed Spam Detection.
d. Reduce Bandwidth Usage by Detection Un-related Video.

Fig. 3 Work Flowchart

CONCLUSION

In this paper, we presented a method based on the type specification of video for detection of the video responses spam on video sharing web sites. The proposed method detects the spam for responded videos and categorize accordingly such as porn, commercial and botnet videos. The detection is based on some parameters such as title, description, uploaded time, likes, etc. The survey shows that the likes for commercial and porn videos are approximately zero because of privacy and upload time is less for botnet video because it can be uploaded by the script. The web sites has been developed for implement the spam methods and results shows the un-related and related videos. This filtration has been performed based on features of video and responds video. The dictionary for commercial and porn words has been generated in database and compared it with the video features. The proposed method is efficient because the words dictionary can be update and will be helpful for spam detection and will be prevented by uploaded of irrelevant data.

REFERNCES

[1] Andras A. Benczur, Karoly Csalogany, Tamas Sarlas, Mate Uher (2002), "SpamRank-Fully Automatic Link Spam Detection".
[2] Helen Costa UFOP, Fabricio Benevenuto, Luiz H. C. Merschmann(2003), "Detecting Tip Spam in Location-based Social Networks".
[3] Gilad Mishne, David Carmel, Ronny Lempel (2005), "Blocking Blog Spam with Language Model Disagreement".
[4] Luca Becchetti, Carlos Castillo Debora, DonatoAdriano Fazzone, (2006), "A Comparison of Sampling Techniques for Web Graph Characterization".
[5] Seungyeop Han, Yong-yeol Ahn, Sue Moon, Hawoong Jeong(2006), "Collaborative Blog Spam Filtering Using Adaptive Percolation Search".
[6] Yuan Niu Yi-Min Wang Hao Chen Ming Ma Francis Hsu(2006), "A Quantitative Study of Forum Spamming Using Context-based Analysis".
[7] Yuan Niu, Yi-Min Wang (2007), "A Quantitative Study of Forum Spamming Using Context-based Analysis", Network & Distributed System Security.
[8] Alan Mislove Massimiliano Marcon Krishna P. Gummadi (2007), "Measurement and Analysis of Online Social Networks", ACM.
[9] Haifeng Yu, Michael Kaminsky, Phillip B. Gibbons, Member, IEEE, and Abraham D. Flaxman(2008), "SybilGuard: Defending Against Sybil Attacks via Social Networks".
[10] Fabricio Benevenuto Fernando Duarte (2008) ,"Understanding Video Interactions In Youtube", ACM.