JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지(J. Korea Inst. Inf. Commun. Eng.) Vol. 20, No. 2 : 260~267 Feb. 2016

감성분석과 SVM을 이용한 인터넷 악성댓글 탐지 기법

홍진주 · 김세한 · 박제원 · 최재현*

A Malicious Comments Detection Technique on the Internet using Sentiment Analysis and SVM

Jinju Hong · Sehan Kim · Jeawon Park · Jaehyun Choi*

Graduate School of Software, Soongsil University, Seoul 06978, Korea

요 약

인터넷을 통해 많은 정보를 얻고 많은 정보를 타인에게 제공하면서 개인의 삶의 양식에 큰 변화를 가져다주었다. 모든 사회 현상에는 양면성이 있듯이 인터넷 익명성을 이용하여 명예훼손, 인신공격, 사생활 침해등과 같이 악의적으로 이용하여 사회적으로 심각한 문제를 양산하고 있다. 인터넷 게시판의 악성댓글은 인터넷에서 발생하는 불법적인 언사나 행위와 관련하여 가장 대두되고 있는 문제이다. 이러한 문제를 해결하기 위해 많은 연구가 진행되고 있지만 악성댓글에 사용된 단어들은 변형이 많이 나타나기 때문에 기존 연구들은 이러한 변형된 악성어휘를 인식하는데 한계점이 존재한다. 이에 본 연구에서는 기존 연구의 한계점을 개선하여 악성댓글을 탐지하는 기법을 제안한다. 실험결과 87.8%의 정확도를 나타냈으며, 이는 기존 연구들에 비해 상당히 발전된 결과로 볼 수 있다.

ABSTRACT

The Internet has brought lots of changes to us sharing information mutually. However, as all social symptom have double-sided character, it has serious social problem. Vicious users have been taking advantage of anonymity on the Internet, stating comments aggressively for defamation, personal attacks, privacy violation and more. Malicious comments on the Internet are creating the biggest problem regarding unlawful acts and insults which occur on the Internet. In order to solve the issues, several studies have been done to efficiently manage the comments. However, there are limitations to recognize modified malicious vocabulary in previous research. So, in this paper, we propose a malicious comments detection technique by improving limitation of previous studies. The experimental result has shown accuracy of 87.8% providing higher accuracy as compared to previous studies done.

키워드 : 데이터 마이닝, 악성댓글, SVM, 감성분석, 한글 정규화

Key word : data mining, malicious comments, SVM, sentiment analysis, Korean normalization

Received 23 December 2015, **Revised** 13 January 2016, **Accepted** 27 January 2016

*** Corresponding Author** Jaehyun Choi(E-mail:jaehyun@ssu.ac.kr, Tel:+82-2-828-7018)
Graduate School of Software, Soongsil University, Seoul 06978, Korea

Open Access http://dx.doi.org/10.6109/jkiice.2016.20.2.260 print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

2014년 7월 현재 우리나라의 인터넷 이용자 수가 4천만 명을 넘어선 것으로 나타났다[1]. 만 3세 이상 인구의 83.6%가 이용하고 있다는 것은 이미 인터넷이 우리 사회에 보편화되어 있음을 나타낸다. 인터넷은 사용자들에게 다양한 정보를 제공하여 사람들의 삶의 양식에 큰 변화를 주었다. 모든 사회 현상에는 양면성이 있듯이 인터넷 이용의 확산은 우리 사회에 긍정적으로만 작용하는 것은 아니다. 인터넷 익명성을 이용하여 명예훼손, 인신공격, 사생활 침해 등과 같이 악의적으로 이용하여 사회적으로 심각한 문제를 양산하고 있다. 인터넷 게시판의 악성댓글은 인터넷에서 발생하는 불법적인 언사나 행위와 관련하여 가장 대두되고 있는 문제이다. 댓글은 인터넷에 게시된 원문기사에 대하여 또 다른 정보나 의견을 답하여 올리는 글이며, 악성댓글이란 인터넷의 익명성을 악용하여 상습적으로 남을 헐뜯거나 허위 사실을 퍼뜨리는 댓글을 말한다[2].

악성댓글로 인한 피해가 확산되면서 정부에서는 이를 해결하기 위한 움직임이 일찍부터 있어왔다. 악성댓글의 원인 중 하나인 익명성을 해결하기 위하여 2007년 ‘인터넷 제한적 본인확인제’를 도입하였으나, 2012년 8월 헌법재판소는 인터넷 제한적 본인확인제가 과잉금지원칙에 위반하여 표현의 자유와 언론의 자유 등과 같은 기본권을 침해한다는 이유로 위헌 판결을 내렸다[3].

또한, 방송통신심의위원회는 현정부 국정과제 중에서 ‘세계 최고의 인터넷피해구제센터’를 개소하여 운영중이지만 인력이 충분하지 않고 홍보도 제대로 이루어지지 않고 있다[4]. 이렇게 악성댓글을 근절하기 위한 정부에서의 시도가 효과를 보지 못하는 가운데 악의적인 댓글을 시스템적으로 관리하기 위한 많은 연구들이 진행되었지만 악성댓글을 작성하는 사용자는 기존의 문법을 파괴하면서 댓글을 작성하기 때문에 변형된 악성어휘를 인식하는데 취약하다는 단점이 존재한다. 이에 본 연구의 목적은 기존 연구들의 한계점을 개선하여 인터넷상에서 작성되는 방대한 양의 데이터 중에서 악의적인 정보를 탐지하는 정확도를 높여 건전한 사이버 생태계를 구현하는데 기여할 수 있는 기법을 제안하고자 한다.

Ⅱ. 관련 연구

2.1. 한글 정규화 기법

악성댓글은 악성 어휘로 차단되는 것을 피하기 위해 인위적으로 변형된 한글을 사용하고 있다. 악성댓글의 데이터를 살펴보면 욕설 사이에 특수 기호들을 삽입하거나 한글로 대체할 만한 특수문자, 숫자, 그리고 영문자를 한글대신 사용하고 있다. ‘ㅈ1랄’과 같이 자음과 모음을 분리한다든지, ‘ㅈ1랄’과 같이 분리된 모음을 유사한 형태의 영문자, 숫자로 변경하여 악성어휘로 인식되지 않도록 교묘한 방법들이 사용되고 있다. 또한, 인터넷 댓글은 한글 띄어쓰기 규칙을 지키지 않고 고의로 공백들을 삽입하거나 ‘쓰.레.기.들’과 같이 각 문자들 사이에 특수문자 등 문자부호를 삽입하는 형태로 왜곡하기도 한다. 이와 같이 모음과 자음을 분리하거나 유사한 특수문자로 변경하는 방법에 의해 하나의 어휘는 다양한 형태로 문자열 조합이 가능하다[5]. 특히 기계는 사람과 달리 편집된 글의 의미를 인식하지 못하여 욕설 및 비속어가 포함된 댓글을 필터링 하는데 한계가 존재한다. 이에 본 연구에서는 [5]의 연구 방법을 바탕으로 변형된 한글을 정상적인 한글로 복원하는 연구를 진행한다.

2.2. 감성분석

감성분석이란 사용자가 작성한 문장의 성향을 나타내는 패턴을 이용해 텍스트 내에서 주관적인 정보를 검토하고 처리하는 기법으로 기본 작업은 문장의 극성을 긍정, 부정, 중립 등으로 나누는 것이다. 하지만 본 논문에서는 감성분석을 악성댓글을 분류하는 것에 이용하지 않고 기계학습 알고리즘 중 하나인 SVM(Support Vector Machine)을 이용해 학습시키기 위한 데이터의 속성으로 사용하고자 한다. 감성분석의 과정은 형태소 분석기를 사용해 텍스트를 분해하고 추출한 단어를 감성사전과의 비교를 통해 텍스트의 단어 빈도수와 악성지수를 도출하는 과정까지만 진행한다.

2.3. 감성사전

감성사전을 구축하기 위해 수집한 댓글을 형태소 단위로 분석해야한다. 형태소는 언어학에서 일정한 의미가 있는 최소단위이며, 형태소 분석이란 문장을 구성하고 있는 각각의 마디를 형태소로 분리한 후 각 형태소

에 맞는 범주를 부여하는 과정이다[6]. 본 연구는 서울대학교 IDS(Intelligent Data System) 연구실에서 개발한 '꼬꼬마 형태소 분석기'를 이용하여 수집한 댓글의 형태소 분석을 진행한다. [7]의 연구는 도메인의 특성을 고려하여 구축한 감성사전을 감성평가에 이용함으로써 정확도를 향상시켰고, [8]에서도 특화된 감성사전을 구축하여 이를 감성분류에 사용함으로써 정확도가 높게 나타났다. 댓글에는 비속어나 은어가 많이 쓰이기 때문에 댓글의 정확한 감성분석을 위해 비속어나 은어들을 고려해야 함으로 본 연구에서는 [9]의 방법을 이용하여 악성댓글을 탐지하기 위해 특화된 감성사전을 구축하고, 구축된 감성사전을 통해 댓글의 감성을 분석한다. [9]의 방법은 단어의 긍정지수를 0~1까지의 수로 산출하였다면, 본 논문은 [9]의 방법과 동일한 식을 이용하여 단어의 악성지수를 0~1까지의 수로 산출하여 분석에 응용하였다.

2.4. SVM(Support Vector Machine)

SVM은 1995년 통계학자인 Vladimir Vapnik와 그의 AT&T Bell 연구소 팀에 의해 개발된 두 범주의 패턴 인식 문제를 해결하기 위해 소개된 학습기법이다[10]. SVM의 기본 원리는 두 개의 범주로 구성된 N개의 점이 하나의 분리경계면(Hyperplane)으로 구분이 될 때, 두 범주를 구분하는 분리경계면은 무수히 많을 수 있으나 SVM은 지지벡터(Support Vector)라고 하는 특정한 점들에 의해 결정되는 두 그룹간의 마진(Margin)을 최대로 하는 분리경계면을 통해 두 그룹으로 구분한다. 분리경계면에서 가장 가까운 데이터들을 지지벡터라고 부른다. 지지벡터는 분리경계면을 결정하는 중요한 정보이다. 분리경계면을 수식으로 표현하면 $y = wx + b = 0$과 같다. w와 b는 학습으로부터 얻어진 결과이며 x는 구분하려고 하는 데이터의 벡터이다. 학습 데이터가 A범주와 B범주로 나누어진다고 가정했을 때, SVM을 학습시킨 후 새로운 객체 x에 대한 분류규칙은 $y = wx + b > 0$이면 범주 A, $y = wx + b < 0$이면 범주 B로 분류된다.

2.5. 악성댓글 탐지를 위한 기존 연구

악성댓글 탐지에 관한 연구는 온라인 뉴스기사, 블로그, SNS를 중심으로 이루어져왔다. 댓글에 대한 키워드 기반의 사전을 형성하여 탐지하는 방법에서 기계학습 알고리즘을 이용한 방법으로 발전하였다. [11]은 포탈사이트의 뉴스에 대한 댓글을 형태소 분석기를 이용하여 단어를 추출하고 단어의 품사 정보를 조합하여 단어의 출현빈도(Term Frequency : TF)와 역 문헌빈도(Inverse Document Frequency : IDF)의 가중치를 계산하여 SVM 알고리즘으로 악성댓글 여부를 판단하는 시스템을 제안하였고, [12]는 정치 뉴스 기사를 대상으로 토픽 시그니처를 나이브 베이지안 모델을 이용하여 댓글 탐지 시스템을 구현하였다. 또한 [13]은 언어파괴 현상으로 인해 동일한 의미를 탐지하지 못하는 문제의 해결을 위해 유니코드를 사용하여 빈도수가 높은 글자는 초성으로 변경한 다음 키워드를 추출하여 SVM과 Random Forest를 이용한 방법을 제안하였으며 SVM을 활용하였을 때 성능이 더 좋은 것을 나타냈다. 그러나 위의 연구들은 댓글에 특수문자를 삽입하거나 변형된 한글을 인식하는데 취약하다는 단점이 있다.

Ⅲ. 인터넷 악성댓글 탐지 기법

SVM을 이용하여 식을 도출하기 위해서는 미리 학습된 데이터가 필요하다. 학습데이터 500개를 SVM을 사용해 악성댓글을 탐지하기 위한 식을 도출하고, 평가데이터 100개를 이용하여 악성댓글 탐지에 대한 성능을 평가한다. 본 논문에서 제안하는 기법의 과정은 그림 1과 같다.

3.1. 데이터 수집

실험에 필요한 데이터는 페이스북의 댓글을 수집해주는 'the fancake서비스[14]'를 사용한다. 500개의 학습데이터와 100개의 평가데이터를 수집하였으며 수집된 댓글은 수작업으로 악성댓글과 일반댓글로 구분한다. 뉴스 기사의 댓글은 작성자의 의도에 따라 기사의 내용에 대해 자신의 소감, 주장, 견해 등을 표현하는 사실판단형과 자신의 내적인 감정을 표현하는 감정발산형이있다[15]. 감정발산형 댓글은 기사 내용에 대해 응원하는 댓글을 작성하기도 하지만, 비속어와 욕설을 사용함으로써 폭력적인 언어를 사용하기도 한다. 따라서 본 연구는 욕설이나 비속어를 사용하거나 상대방이 불쾌감을 느낄 부정적인 언어를 사용하는 댓글을 악성댓글로 구분한다.

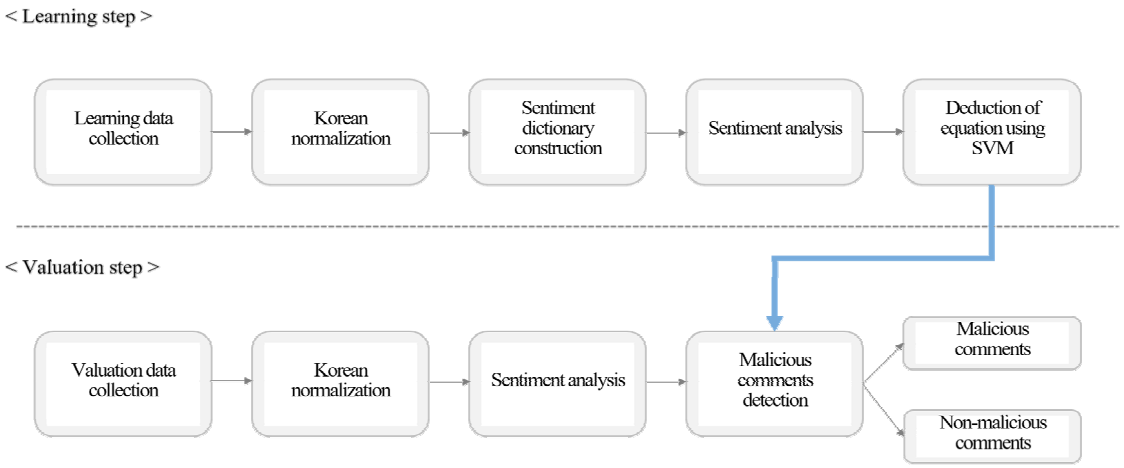

Fig. 1 overall process of suggested technique

3.2. 한글 정규화

악성댓글은 악성어휘로 차단되는 것을 피하기 위해 인위적으로 변형된 한글을 사용하고 있다. 이에 본 논문은 [5]의 연구를 바탕으로 변형된 한글을 정상적인 한글로 복원하는 연구를 진행한다. 한글 정규화 과정은 그림 2와 같다.

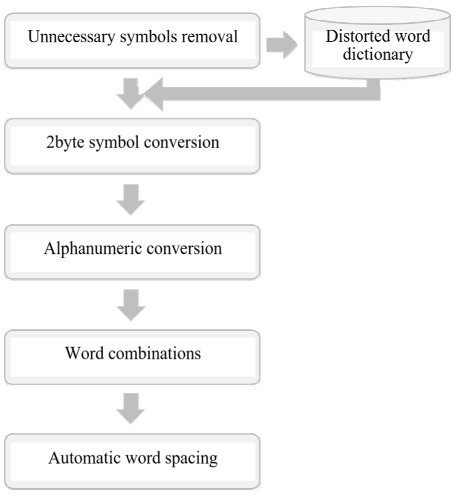

Fig. 2 process of Korean normalization

한글 정규화의 첫 번째 단계는 공백 문자 등 불필요한 기호들을 제거한다. 두 번째 단계는 모음이 모두 누락된 단어들을 미리 사전에 등록하여 변형 문자열이 있을 경우 사전에 등록된 문자열을 복원한다. 세 번째 단계는 자음 'ㅇ'를 특수문자 '@'로 대치하거나 또는 숫자나 영문자 '0/o'로 대치하는 경우가 많아 다양한 형태로 변형된 한글을 정상적인 한글로 대치한다. 그 다음, 자모가 분리되는 유형들에 대해 정상적인 한글 문장으로 복원한다[5]. 마지막으로 변환 과정을 거친 문장은 공백이 무시되어있으므로 자동 띄어쓰기 모듈을 적용한다[16].

3.3. 감성사전 구축

감성사전은 댓글의 악성을 분석하는 과정에서 사용하는데, 분석의 정확도를 높이는데 매우 큰 비중을 차지한다. 기존 연구에서는 악성댓글에 특화된 감성사전이 구축되어있지 않아 본 논문에서는 [9]의 긍정지수를 산출하는 방법을 바탕으로 악성댓글에 특화된 감성사전을 구축하여 악성지수를 산출하는 연구를 진행한다. 한글 정규화 과정을 거친 댓글은 형태소를 분석하여 감성사전에 등록할 후보 단어들을 추출한다. 이때 사용되는 형태소 분석기는 서울대학교에서 개발한 '꼬꼬마 형태소 분석기'를 사용한다. 형태소 분석을 통해서 추출된 단어들은 빈도수와 악성 값을 계산하는데, 이때 빈도수는 해당 단어가 나온 댓글의 수를 합산하여 계산하고, 악성 값은 해당 단어가 들어간 댓글이 악성댓글일 경우의 수를 합산하여 계산한다. 빈도수($frequency$)를 수식으로 나타내면 식 (2)와 같으며, 악성 값(Malicious Value, MV)은 식 (4)와 같다.

$$include(i,j)=\begin{cases}1\ (\text{댓글 } j\text{에 단어 } i\text{가 포함된 경우})\\ 0\ (\text{그 외의 경우})\end{cases} \quad (1)$$

$$frequency(i)=\sum_{j=1}^{n} include(i,j) \quad (2)$$
$n=$ 전체 댓글의 수

$$M(j)=\begin{cases}1\ (\text{댓글 } j\text{가 악성일 경우})\\ 0\ (\text{그 외의 경우})\end{cases} \quad (3)$$

$$MV(i)=\sum_{j=1}^{n}\{include(i,j)\times M(j)\} \quad (4)$$
$n=$ 전체 댓글의 수

감성사전에는 단어와 단어의 빈도수, 악성지수를 계산하여 감성사전을 완성한다. 악성지수(Malicious index, MI)는 악성 값을 빈도수로 나누어 나타내며, 0에서 1사이의 값으로 1에 가까울수록 악성의 의미를 나타낸다. 식으로 표현하면 식 (5)와 같다.

$$MI(i)=\frac{\sum_{j=1}^{n}\{include(i,j)\times M(j)\}}{\sum_{j=1}^{n} include(i,j)} \quad (5)$$
$n=$ 전체 댓글의 수

3.4. 감성사전을 통한 댓글의 감성분석

구축한 감성사전을 활용하여 댓글의 감성분석을 진행한다. 감성분석의 기본 작업은 문장의 극성을 긍정, 부정, 중립 등으로 나누는 것이다. 하지만 본 논문에서는 감성분석을 악성댓글을 분류하는 것에 이용하지 않고 SVM을 이용해 학습시키기 위한 데이터의 속성으로 사용하고자 한다. 댓글의 형태소를 분석하여 단어를 추출한 후, 추출한 단어와 감성사전의 단어들을 비교해 해당 댓글의 악성지수를 계산한다. 댓글의 악성지수(Malicious index of Comment, MC)는 해당 댓글에서 추출한 단어들의 악성지수를 합해 그 개수로 나눈 산술평균값이며, 수식으로 표현하면 식 (7)과 같다.

$$match(i,j)=\begin{cases}1\ (\text{댓글 } i\text{에 포함된 단어 } j\text{가}\\ \text{감성사전에 존재할 경우})\\ 0\ (\text{그 외의 경우})\end{cases} \quad (6)$$

$$MC(i)=\frac{\sum_{j=1}^{n}\{match(i,j)\times MI(j)\}}{\sum_{j=1}^{n} match(i,j)} \quad (7)$$
$n=$ 댓글 i에 포함된 단어의 수

댓글의 단어 빈도수와 악성지수를 도출한 후 악성댓글 여부 항목을 추가해 SVM을 이용해 학습을 위한 데이터로 사용한다. 악성댓글 여부는 악성댓글일 경우는 yes, 그렇지 않을 경우는 no 두 가지로 나타낸다.

3.5. SVM을 이용한 식 도출

본 논문은 악성댓글을 탐지하기 위해 SVM을 사용하여 최적의 경계면의 식을 도출한다. SVM은 주어진 데이터가 선형으로 분류되는 경우와 분류되지 않을 경우 적용하는 기법이 다르다. 본 논문에서 사용한 데이터는 비선형 SVM을 사용하였다. 비선형 SVM의 경우 커널함수를 사용하여 기존 데이터를 고차원 공간으로 변환한 다음, 선형 SVM의 공식화를 통해 2차 계획법 문제로 표현하여 최대 마진 초평면을 찾을 수 있다. 본 논문은 SVM을 학습하는 과정에서 Polynomial kernel를 사용하였고 10-fold cross-validation 방식을 통해 판별 정확도를 입증했다. SVM은 뉴질랜드 와이카토 대학에서 개발한 오픈소스 소프트웨어인 'WEKA'를 사용하였다. 500개의 학습 데이터를 이용해 y=0.2875a+5.4685b-2.8237 라는 분리경계면 식을 도출하였으며, 이때 데이터의 속성집합에서 a는 댓글의 빈도수, b는 악성지수를 나타낸다. 이 식에 데이터를 대입하여 나온 최종 값은 y>0일 경우 악성댓글, y<0일 경우 일반댓글로 탐지된다.

Ⅳ. 실험결과 및 분석

학습데이터로 교차 검증 절차를 통해 최적화된 SVM을 통한 악성댓글 탐지 식을 도출하고, 평가 데이터로 도출된 식 y=0.2875a+5.4685b-2.8237 에 대입하여 나온 최종 값들에 근거하여 정확도($Precision$), 재현율($Recall$), 그리고 $F_1-measure$를 계산하여 기법에 대한 성능을 평가하였다. 각각의 대한 정의는 식 (8), (9), (10)과 같다.

$$Precision = \frac{\text{정확히 분류한 실제 악성댓글의 개수}}{\text{분류한 전체 악성댓글의 개수}} \quad (8)$$

$$Recall = \frac{\text{정확히 분류한 실제 악성댓글의 개수}}{\text{실제 댓글의 총 개수}} \quad (9)$$

$$F_1 - measure = \frac{2 \times Precision \times Recall}{Precision + Recall} \quad (10)$$

본 실험에서 탐지 기법의 성능을 평가하기 위하여 학습 데이터 수를 100개에서 300개, 그리고 500개로 증가했을 경우의 탐지 결과를 측정하였고 아래 표와 같은 결과를 얻을 수 있었다.

Table. 1 performance of The proposed method

# of data	Precision	Recall	F1-measure
100	86%	86%	86%
300	86.3%	86%	86.15%
500	87.8%	86%	86.9%

표 1에서 볼 수 있듯이 SVM을 통해 구한 식은 500개의 데이터로 학습했을 때 정확도 87.8%와 재현율 86%, 그리고 $F_1 - measure$ 86.9%로 가장 좋은 결과를 나타내었다. 데이터의 개수가 증가함에 따라 성능 면에서 향상된 결과를 보인 것은 보다 많은 양의 데이터를 수집하여 분석한다면 지금보다 더 향상된 결과를 얻을 수 있을 것이라 생각된다. 본 논문에서는 선행연구보다 정확도를 높이는 것을 목표로 하였다. 표 2과 같이 기존의 연구들과 비교했을 때 악성댓글을 탐지하는 정확도가 높아 우수한 성능을 확인하였다.

Table. 2 performance comparison result

Precision	
[11]	65.52%
[12]	75.3%
[13]	78.6%
proposed technique	87.8%

Ⅴ. 결 론

인터넷에서 문제가 되고 있는 악성댓글은 작성자들이 상대방을 배려하지 않는 어휘를 사용함으로써 상대방을 비방하고 공격한다. 이러한 행동에 대해 반성이나 잘못의 인식이 요구되고 있지만 해를 거듭할수록 악성댓글로 인한 피해는 오히려 기하급수적으로 증가하고 있다. 이를 해결하기 위해 본 논문에서는 악성댓글을 탐지하는 기법을 제시하였다. 최근 댓글들은 인위적으로 조작하여 변형된 한글을 사용하기 때문에 한글 정규화 과정을 통해 변형된 한글을 원래의 한글로 복원하였다. 또한 인터넷 댓글에 특화된 감성사전을 구축하였고, 구축된 감성사전을 이용해 댓글의 감성을 분석하였다. 이를 기계학습 알고리즘 중 하나인 SVM을 사용하여 악성댓글 탐지를 위한 하나의 방정식을 도출하였다. 그 후 평가 데이터를 이용하여 정확도($Precision$), 재현율($Recall$), 그리고 $F_1 - measure$을 계산하여 악성댓글 탐지 기법에 대한 성능을 측정하였고, 그 결과 기존의 연구들 보다 정확도($Precision$)가 높아 우수한 성능을 보였다. 본 연구는 기계학습을 시키기 위해 필요한 데이터를 정제하는 과정에서 댓글에 특화된 감성사전을 구축하여 이를 감성분석에 이용할 수 있음을 나타내었다. 또한 실무적으로 기존의 방식에 비해 인위적으로 변형시킨 악성댓글에 대한 탐지 효율이 높을 것이며 이를 더욱 발전시키고 보완한다면 서비스에 적용할 수 있을 것이라고 생각된다. 하지만 감성사전을 구축하는데 필요한 데이터가 충분하지 못하였고 악성댓글의 특징은 시대가 변하면서 계속 변형되고 새로 만들어지기 때문에 새로 생기는 단어들을 일일이 추가하여야 한다는 한계점이 존재한다. 또한 언어의 특징에서 발생되는 여러 가지 문맥적 의미 변이와 반어법 등 문장의 감성을 탐지하기 위해서는 다양한 상황에 대한 고려가 필요하다. 향후 연구에서는 충분한 양의 데이터를 수집하여 감성사전의 지속적인 버전 업을 통해 감성단어의 정확성을 높이는 것이 향후 과제 중 하나이며, 텍스트의 감성을 보다 정확하게 탐지하기 위해 문장에서 단어들 간의 연관성과 문장 규칙을 적용하여 분석한다면 기법의 한계점을 보완할 수 있을 것이다.

REFERENCES

[1] Korean Internet & Security Agency, “Internet Use Survey Summary Report,” Korean Internet & Security Agency (KISA), 2014.

[2] Comments, [Internet]. Available: https://ko.wikipedia.org/wiki/.
[3] E. J. No, “The Constitutional Study on Internet Comments,” a master's thesis SungKyunKwan University, Aug. 2014.
[4] Prosecution service, Internet malicious comments illegal act processing method implementation press release, Apr. 2015.
[5] S. S. Kang, “A Normalization Method of Distorted Korean SMS Sentences for Spam Message Filtering,” *Korea Information Processing Society,* vol. 3, no. 7, pp.271-276, Jul. 2014.
[6] K. S. Shim and J. H. Yang, "High Speed Korean Morphological Analysis based on Adjacency Condition Check," *Korean Institute of Information Scientists and Engineers,* vol. 31, no. 1, pp.89-99, Jan. 2004.
[7] J. S. Song and S. W. Lee, "Automatic Construction of Positive/Negative Feature-Predicate Dictionary for Polarity Classification of Product Reviews," *Korean Institute of Information Scientists and Engineers,* vol. 38, no. 3, pp.157-168, Mar. 2011.
[8] S. W. Kim and N. K. Kim, “A Study on the Effect of Using Sentiment Lexicon in Opinion Classification,” *Korea Intelligent Information System Society,* vol. 20, no. 1, pp.133-148, Mar. 2014.
[9] E. J. You, Y. S. Kim, N. K. Kim and S, Y. Jung, “Predicting the Direction of the Stock Index by Using a Domain-Specific Sentiment Dictionary,” *Korea Intelligent Information System Society,* vol. 19, no. 1, pp.95-110, Mar. 2013.
[10] Corinna Cortes and Vladimir Vapnik, "Support vector networks," *Machine Learning 20*, pp.273-297, 1995.
[11] M. S. Kim and S. S. Kang, “A Design and Implementation of Malicious Web Log Identification System by Using SVM,” *18st Annual Conference on Human and Language Technology*, pp.285-289, Oct. 2006.
[12] M. Y. Bae and J. W. Cha, “Comments Classification System using Topic Signature,” *Korean Institute of Information Scientists and Engineers*, vol. 35, no. 12, pp.774-779, Dec. 2008.
[13] H. J. Kim, Y. M. Yoon and B. M. Lee, “Prediction System for Abusive Postings using Enhanced FFP,” *Journal of Korean Institute of Information Technology,* vol. 9, no. 1. pp.207- 216, Jan. 2011.
[14] the fancake, [Internet]. Available: https://thefancake.co.kr/
[15] K. H. Joe, “A Study Text Typological of Internet Comments,” *The Textlinguistic Society of Korea,* vol. 23, pp.203-230, Nov. 2007.
[16] S. S. Kang and K. B. Hwang, "A Language Independent n-gram Model for Word Segmentation," *Advances in Artificial Intelligence 2006,* vol. 4303, pp.557- 565, Dec. 2006.

홍진주(Jinju Hong)

2014년 3월~현재 숭실대학교 SW특성화대학원 공학석사
※관심분야 : 데이터마이닝, 빅 데이터, 서비스엔지니어링

김세한(Sehan Kim)

2015년 3월~현재 숭실대학교 SW특성화대학원 공학석사
※관심분야 : 데이터마이닝, DB설계 및 모델링, IoT

박제원(Jeawon Park)

2006 년 2월 숭실대학교 대학원 컴퓨터학과 석사
20011년 8월 숭실대학교 대학원 컴퓨터학과 박사
2012 년 2월~2013년 2월 숭실대학교 SW특성화대학원 연구교수
2013년~현재 숭실대학교 SW특성화대학원 교수
※관심분야 : 소프트웨어공학, 정보보호, SW품질보증, 오픈소스소프트웨어 등

최재현(Jaehyun Choi)

2006년 2월 숭실대학교 대학원 컴퓨터학과 석사
2012년 2월 숭실대학교 대학원 컴퓨터학과 박사
2012 년 2월~2013년 2월 숭실대학교 SW특성화대학원 연구교수
2013년~현재 숭실대학교 SW특성화대학원 교수
※관심분야 : 소프트웨어공학, 정보보호, SW품질보증 등