Journal of Digital Contents Society Vol. 16 No. 5 Oct. 2015(pp. 815-822)
http://dx.doi.org/10.9728/dcs.2015.16.5.815

집합 기반 POI 검색 알고리즘을 활용한 스팸 메시지 판별 모바일 앱 구현

안혜영*, 조완지**, 이종우***

요 약

최근 스미싱 피해가 늘어남에 따라 스팸 메시지 처리를 위한 애플리케이션이 잇달아 출시되고 있다. 그러나 자음과 모음을 분리하는 등 교묘하게 내용이 조작된 스팸 메시지는 필터링하지 못 하는 경우가 대부분이다. 이를 해결하기 위해 본 논문에서는 문자 메시지 내 스팸 문자열을 검사하는 애플리케이션인 안티스팸을 구현하였다. 안티스팸은 집합 기반 POI 검색 알고리즘을 활용하여, 전송된 문자 메시지 내에 스팸 문자열이 있는지 검색한 후, 검색 결과에 따라 스팸 여부를 추정한다. 또한 스팸 필터링을 피하기 위해 교묘히 위장된 스팸 메시지도 걸러준다. 사용자는 메시지를 받으면 스팸 판단 결과와 메시지 내용을 확인하고 메시지 처리방식을 선택할 수 있다.

키워드 : 스팸, 필터링, 문자메시지, 안드로이드

Implementation of A Mobile Application for Spam SMS Filtering Using Set-Based POI Search Algorithm

Hye-yeong Ahn*, Wan-zee Cho**, Jong-woo Lee***

Abstract

By the growing of SMS phishing victims, applications for processing spam messages are being released in succession. However most spam messages that cleverly modified the content like separating the consonants and vowels are fail to be filtered. In this paper, we implemented an application 'AntiSpam' which is able to identify spam strings in the text message to solve this problem. 'AntiSpam' searches spam strings in the text message by using set-based POI search algorithm, and then calculate the possibility of whether it is spam or not in accordance with the search results. In addition, it catches skillfully disguised spam messages in order to avoid missing the spam filtering. Users, who received a message, can check the result in spam message possibility decision result and the contents of the message and they can choose how to handling the message.

Keywords : Spam, Filtering, Text Message, Android

1. 서론

휴대폰은 오래 전부터 우리 생활의 필수품이 되었다. 사람들은 휴대폰의 메시지 기능을 통해 편리하고 빠르게 서로 연락을 주고받는다. 그러

※ Corresponding Author : Jong-woo Lee
Received: September 01, 2015
Revised: October 30, 2015
Accepted: October 31,, 2015
* Sookmyung Women's University Multimedia Science
Tel: +82-10-4900-2617
email: hyeyeong@sookmyung.ac.kr
** Sookmyung Women's University Multimedia Science
email: wonzee@naver.com
*** Sookmyung Women's University Multimedia Science
email: bigrain@sookmyung.ac.kr
▣ 이 논문은 2015년도 정부(교육부)의 재원으로 한국연구재단 기초연구사업 지원을 받아 수행된 것임 (NRF-2013R1A1A2013155)
▣ 본 연구는 숙명여자대학교 교내연구비지원에 의해 수행되었음(과제번호 1-1503-0169)

나 불특정 다수에게 광고 등을 전송하는 스팸 메시지에도 쉽게 노출되고 있다. 이를 막기 위하여 통신사에서 스팸 메시지를 일차적으로 검사하지만, 스팸 문자열의 자음과 모음을 분리하거나 문자열 중간에 특수문자를 삽입하는 등 교묘하게 조작된 스팸 메시지까지 걸러내기에는 역부족인 실정이다.

본 논문에서는 이러한 문제점을 해결하기 위해 문자 메시지 내의 스팸 문자열을 찾아 스팸 메시지 여부를 판별하는 애플리케이션인 안티스팸(AntiSpam)을 설계하고 구현하였다. 안티스팸은 집합 기반 POI(Point Of Interest) 검색 알고리즘[1]을 활용하여 문자 메시지 내의 스팸 문자열을 검사한다. 집합 기반 POI 검색 알고리즘을 특수 문자와 섞여 있거나 세로로 숨겨져 있는 등 변형된 스팸 메시지 내의 스팸 문자열 검색에 활용한 것이다. 집합 기반 POI 검색 알고리즘을 통해 검색된 결과를 토대로 스팸 메시지 여부를 메시지 수신 시 실시간으로 제공한다. 팝업 화면에서 문자 메시지를 확인하고 스팸 메시지일 경우 바로 삭제할 수 있다.

본 논문의 구성은 다음과 같다. 2장에서는 현재 스마트폰에서 사용되고 있는 스팸 처리 애플리케이션과 기존 스팸 필터링 알고리즘에 대하여 살펴본 후, 본 논문에서 활용한 집합 기반 POI 검색 알고리즘에 관해 기술한다. 3장에서는 안티스팸의 설계 및 구현 내용을 기술하고, 4장에서 애플리케이션의 실행 화면을 보인다. 5장에서는 안티스팸과 기존 스팸 차단 애플리케이션과의 비교를 통해 성능을 평가하고, 마지막 6장에서는 결론을 제시한다.

2. 관련연구

2.1 기존 스팸 차단 애플리케이션 분석

기존 스팸 문자 및 전화 차단 애플리케이션들은 발신 번호를 기반으로 스팸을 차단한다. 또한 전화번호로 완벽히 차단되지 않을 경우를 대비하여 사용자가 직접 스팸 문자열 등록을 할 수 있도록 지원한다.

특히 통신사에서 제공하는 스팸 차단 애플리케이션은 통신사 서버에 저장되어 있는 스팸 전화번호와 스팸 문구 정보를 이용하여 스팸을 차단한다. 통신사 서버에 없는 번호나 문구로 스팸 메시지가 올 경우 사용자가 직접 차단 문구로 등록할 수 있다. (그림 1)은 KT에서 제공하는 스팸 차단 애플리케이션의 실행 화면이다.

(그림 1) KT 스팸 차단 애플리케이션

(Figure 1) KT Spam Block Application

통신사에서 제공하는 스팸 메시지 차단 서비스는 데이터베이스가 방대하다는 장점이 있다. 그러나 서버에 있는 또는 사용자가 등록한 문구가 스팸 문자 메시지 내의 문구와 정확히 일치(hard matching)해야 차단이 가능하므로, 자음과 모음을 분리한 문구나 세로로 숨겨져 있는 스팸 문구일 경우에는 차단이 불가능하다.

2.2 기존 스팸 차단 애플리케이션 분석

스팸 필터링에 대한 기존 연구로는 대표적으로 통계적 방법을 이용하는 방법이 있다. 나이브 베이지안 분류자 알고리즘을 활용한 스팸 메일 필터링[2,3]의 경우 학습한 데이터를 토대로 자동으로 스팸 메일을 분류한다. 스팸 메일 또는 메시지는 더욱 교묘하게 진화하므로 새로운 데이터에 대한 빈번한 재학습이 필요하며 숨어있는 스팸 단어를 인지하는 능력이 떨어진다.

이외에도 집단 지성을 이용한 스팸 메시지 필터링 기법[4] 등이 있으나 완전한 단어 형태의 스팸 문자열이 기반이 되므로 변형된 스팸 메시지에 대한 처리가 부족하다.

2.3 집합 기반 POI 검색 알고리즘

집합 기반 POI(Point Of Interest) 검색 알고리즘은 별도의 서버 등 외부 자원을 사용하지 않고도 쿼리를 알고리즘 차원으로 재구성하므로, 오·탈자나 외래어 표기법에 의한 잘못된 입력

등 부정확한 쿼리에 대한 처리가 가능하다[5].

집합 기반 POI 검색 알고리즘의 원리는 다음과 같다. n개의 문자로 이루어진 POI 쿼리를 m개의 블록으로 균등 분할한다. 각 블록에 대해 집합 기반 연산을 적용 후 '차수'라는 개념을 사용하여 블록 간 집합 연산을 수행한다. 즉, 쿼리 내 문자 집합과 데이터 문자 집합 간의 포함 관계(또는 부분 포함 관계)를 이용하는 것이다.

집합 기반 POI 검색 알고리즘을 활용할 경우 자음과 모음이 분리되어 있거나 세로로 스팸 문자열을 숨겨두는 등 교묘하게 내용을 변형시킨 스팸 문자열을 검색할 수 있다. (그림 2)는 메시지의 내용이 변형된 스팸 문자 메시지의 예이다.

(그림 2) 변형된 스팸 문자 메시지 예

(Figure 2) Modified mobile spam text message examples

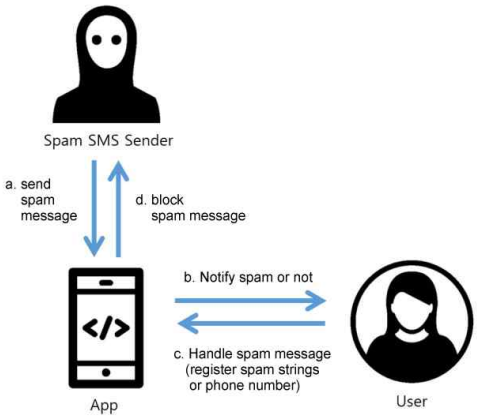
(그림 2)처럼 글자 사이에 특수문자를 추가하거나 줄 바꿈 등을 통해 스팸 문자열 자체를 변형시킨다. 따라서 스팸 문자열이 기반이 되는 하드 매칭 기법 등 기존 스팸 필터링에서는 변형된 단어와 정확하게 일치하는 스팸 문자열이 데이터베이스에 없기 때문에 필터링이 불가능하다.

3. 시스템 설계 및 구현

3.1 시스템 설계

본 논문에서 제안하는 스팸 차단 애플리케이션인 안티스팸은 휴대폰에 수신된 문자의 문자열을 스팸 문자열과 비교하여 스팸 메시지를 판별하는 애플리케이션이다. 스마트폰 내 존재하는 로컬 스팸 문자열 데이터베이스에 있는 문자열과 수신된 문자의 문자열 중 매칭되는 문자열이 있는 지 검사한다. 검사 결과, 매칭이 되는 문자열이 있다면 스팸으로 표시하고 매칭된 문자열의 개수와 정확도 그리고 스팸 문자열의 가중치에 따라 스팸 여부 및 메시지 내에서 검색된 스팸 문자열을 팝업으로 보여준다. 사용자는 이것을 토대로 문자 메시지를 확인하고 넘어갈 것인지 삭제할 것인지 결정한다. 사용자가 스팸이라고 표시하고 싶은 문자열이나 전화번호가 있을 경우 직접 해당 항목을 추가할 수도 있다. (그림 3)은 본 애플리케이션의 실행 흐름을 보이고 있다.

(그림 3) 안티스팸 애플리케이션 실행 흐름



(Figure 3) AntiSpam application's execution flow

3.2 시스템 구현 환경

안티스팸은 안드로이드 운영체제용으로 구현되었으며, 구현에는 안드로이드 SDK를 사용하였다. 또한 본 앱에서 활용하는 집합 기반 POI 검색 알고리즘은 C로 구현되어 있으므로 안드로이드 시스템 라이브러리에 이식이 필요하다. 이를 위하여 NDK(Native Development Kit)[6]를 이용하였다. C로 구현된 집합 기반 POI 알고리즘을 NDK로 컴파일 한 후 JAVA로 작성된 앱 코드와 연동하여 사용한다. NDK를 이용한 컴파일을 위해 Windows에서 리눅스 명령어를 이용할 수 있도록 고안된 Cygwin[7]을 사용하였다.

3.3 시스템 구현 내용

문자 메시지가 스마트폰에 수신됐을 경우, 안티스팸에서 먼저 수신된 문자 메시지를 받아온다. 이 때, 문자 메시지 발신자의 전화번호와 발신 시간, 문자 메시지 내용을 모두 가져온다.

다음으로 문자 메시지를 변환하는 과정을 거친다. 문자 메시지 내에 포함된 공백이나 특수문자를 모두 제거하여 단순 텍스트로 이루어진 문자 메시지로 내용을 변환한다.

변환된 문자 메시지를 토대로 집합 기반 POI 검색 알고리즘을 수행하여 스팸 여부를 판별한다. 안티스팸의 스팸 문자열 데이터베이스는 자체적으로 구축하였으며, 약 200여개의 흔히 등장하는 스팸 문자열이 스마트폰 내 로컬 DB에 등록되어 있다.

스팸 메시지 판별은 각 스팸 문자열에 부여한 스팸 점수를 이용한다. 스팸 점수는 문자열이 일반 문자 메시지 및 스팸 문자 메시지에 사용되는 빈도에 따라 1부터 3까지 부여한다. 일반 문자 메시지에서도 많이 사용되는 스팸 문자열일 경우 가장 낮은 점수인 1을 부여한다. <표 1>은 스팸 점수 선정 기준을 보여준다.

<표 1> 문자열의 스팸 점수 선정 기준

weight	criteria
1	String is used frequently in general message more than spam message.
2	String is used frequently in spam message more than general message.
3	String is only used to spam message or user registered spam string.

<Table 1> String's spam score selection criteria

예를 들어 '선물'의 경우, 스팸 문자에서도 사용되지만 일반 메시지에서 나타나는 빈도가 높으므로 가중치 1을 부여한다. <표 2>는 스팸 점수 선정 기준에 따라 스팸 문자열에 점수를 부여한 예시이다.

<표 2> 스팸 문자열의 스팸 점수 예

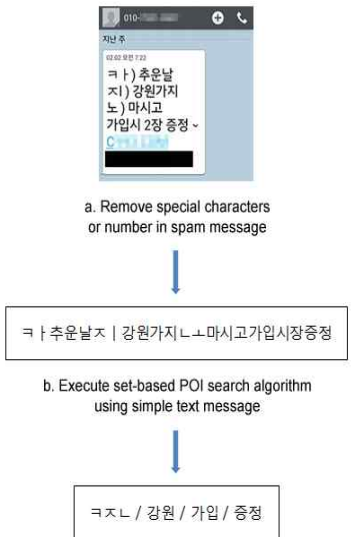
string	spam score
선물	1
현금지원	2
세일	1
바다이야기	3

<Table 2> Examples of spam string score

기존 집합 기반 POI 검색 알고리즘에서 POI 데이터베이스 레코드는 '장소명칭@주소'의 형태로 저장되어 있다. 이를 활용하여 스팸 문자열과 스팸 점수를 함께 저장하기 위해 '스팸 문자열@스팸점수'의 형태로 데이터베이스를 구축하였다.

앞서 문자 메시지를 단순 텍스트 형태로 변환하였고 그 결과에 대해 집합 기반 POI 검색 알고리즘을 이용하여 메시지가 스팸 문자열을 포함하고 있는 지의 여부에 대해 검사하였다. 집합 기반 검색을 통해 검사를 진행하므로 특수 문자가 섞여 있던 스팸 문자열은 물론 초성 형태의 스팸 문자열도 검사가 가능하다. (그림 4)는 스팸 문자열 검사 과정을 보인다.

(그림 4) 스팸 문자열 검사 과정



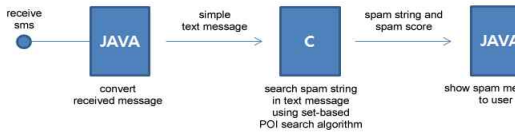
(Figure 4) Spam string inspection process

기존 집합 기반 POI 검색 알고리즘은 단일 프

로그램으로 구현되어 있어 타 프로그램에서 활용이 어려웠다. 이를 쉽게 응용할 수 있도록 기존 시스템을 모듈화하고 API화하여 앱에서 활용하였다.

검사 결과 데이터베이스 내의 스팸 문자열과 일치하는 문자열이 있다면 스팸 키워드와 스팸 점수를 반환 후 스팸 문자열과 문자 메시지의 내용을 함께 사용자에게 보여준다. 이 창을 통해 사용자가 문자를 확인할 것인지 혹은 삭제할 것인지 선택할 수 있다. 스팸 점수는 보안 세기 설정에 사용한다. 보안 세기를 '약'으로 설정했을 경우 스팸 점수가 가장 높은 문자 메시지만 사용자에게 스팸으로 알린다. (그림 5)는 문자 메시지 수신부터 스팸 문자열 검색까지의 실행 흐름을 보여준다.

(그림 5) 안티스팸 실행 흐름도



(Figure 5) AntiSpam's run stream

뿐만 아니라, 사용자가 스팸이라고 판단한 문자열과 전화번호를 앱의 설정을 통해 등록할 수 있다. 이렇게 따로 지정된 문자열과 전화번호를 담고 있는 메시지는 별도 검사 없이 무조건 스팸으로 처리한다.

4. 실행 화면

(그림 6)은 안티스팸의 메인 화면이다. 검사를 켜거나 끌 수 있다.

(그림 6) 스팸 검사 온, 오프 설정 화면

(Figure 6) AntiSpam On/Off set up screen

(그림 7)의 왼쪽 화면은 보안 세기 설정 화면이다. 해당 설정에서는 보안 세기의 강도를 설정할 수 있다. 기본으로 '보통'으로 설정되어 있으며, '보통'으로 설정 시 스팸 점수의 평균이 2 이상일 경우에 스팸으로 알린다. '강함'의 경우에는 스팸 점수 평균이 3 이상, '약함'의 경우에는 스팸 점수 평균이 1 이상일 경우에 스팸으로 알린다.

(그림 7) 보안 세기 설정 화면과 설정 탭 화면

(Figure 7) Security strength setting screen, Setting tab screen

(그림 7)의 오른쪽 화면은 애플리케이션 설정 화면이다. 스팸 문자열과 스팸 번호를 설정할 수 있고 개발자에게 문의 사항을 메일로 전달 할 수 있다.

(그림 8, 9, 10, 11)은 스팸 문자가 수신 되었을 때 사용자의 스마트폰에 보이는 팝업 화면들의 예이다. 문자 메시지를 스팸 메시지로 판별하였으며, 스팸 키워드를 문자 메시지의 내용과 함께 보여준다. 하단의 버튼을 통해 메시지를 확인 또는 삭제를 할 수 있다.

(그림 8) 스팸 키워드를 보여주는 팝업 화면

(Figure 8) A pop-up screen that shows the spam keyword

(그림 9) 스팸 키워드를 보여주는 팝업 화면

(Figure 9) A pop-up screen that shows the spam keyword

(그림 10) 스팸 키워드를 보여주는 팝업 화면

(Figure 10) A pop-up screen that shows the spam keyword

(그림 11) 스팸 키워드를 보여주는 팝업 화면

(Figure 11) A pop-up screen that shows the spam keyword

5. 성능 평가

안티스팸의 성능 검증을 위하여 통신사(KT)와 스팸 전화 및 메시지 차단 애플리케이션과의 스팸 판별 비교를 진행하였다.

통신사의 경우 자체적으로 스팸 메시지 차단 기능을 지원하여 사용자가 아예 스팸 메시지를 수신할 수 없도록 한다. 스팸 전화 및 메시지 차단 애플리케이션의 경우 실시간 감시를 통하여 스팸 전화 또는 스팸 메시지가 수신될 경우 알람을 통하여 알려준다.

성능 평가를 위해 아래와 같은 스팸 문자 메시지를 전송하여 스팸 처리 여부를 확인하였다.

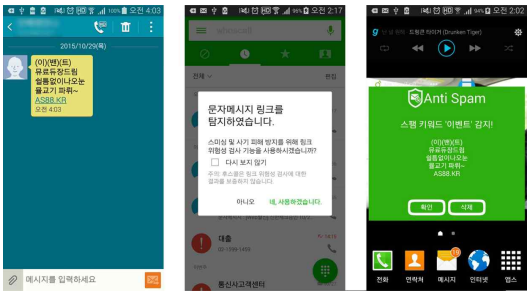
<표 3> 기존 스팸 차단 기능 및 애플리케이션과 안티스팸 간 스팸 차단 여부 비교

spam message / application	<NH농/협>서민지원팀! 최대_4천까지_연7%~기.준완.화~오늘즉/시가능	(이)(밴)(트)뮤료듀장드림쉴틈없이나오눈물교기 파뤄~AS88.KR
KT	처리 못함	처리 못함
spam blocking app (whoscall)	처리 못함	스미싱 메시지로 판단
AntiSpam	처리함	처리함

<Table 3> Comparison between existing spam filtering application and AntiSpam

<표 3>을 통해서 안티스팸은 스팸 단어들 사이에 특수 문자를 추가하는 등 교묘하게 변형한 스팸 메시지 또한 스팸으로 처리하는 것을 알 수 있다. (그림 12)는 <표 3>의 스팸 메시지를 통신사, 스팸 차단 앱과 안티 스팸에서 수신했을 때의 화면이다. 왼쪽부터 순서대로 통신사, 스팸 차단 앱, 안티 스팸의 화면이다.

(그림 12) 애플리케이션 별 스팸 메시지 수신 화면



(Figure 12) Each of screen receiving spam message

안티스팸은 단어 사이에 특수 문자를 추가하거나 '이벤트'라는 단어를 '이밴트'로 사용하는 등 메시지를 변형시켜 전송하는 스팸 메시지 또한 집합 기반 POI 검색 알고리즘을 활용하여 스팸 메시지로 판별하는 것을 확인하였다.

6. 결론 및 향후 연구방향

본 논문에서는 집합 기반 POI 검색 알고리즘을 활용하여 스팸 메시지를 판별할 수 애플리케이션을 설계하고 구현하였다. 기존 스팸 문자 차단 애플리케이션의 경우, 전화번호를 기준으로 차단하는 애플리케이션이 대부분이며 방대한 양의 전화번호 데이터베이스를 토대로 스팸을 차단한다. 그러나 전화번호가 데이터베이스에 없는 경우에는 차단되지 않으며 스팸 번호를 사용자가 직접 등록해야 한다. 또한 문자열을 기준으로 할 경우 데이터베이스에 있는 스팸 문자열과 정확하게 일치할 경우에만 차단이 되는 문제점이 있다. 차단을 피하기 위하여 스팸 문자열의 자음과 모음을 분리하거나 세로로 스팸 문자열을 숨겨두는 등 스팸 메시지의 내용을 조작하여 보낸다.

이러한 문제점을 해결하기 위하여 본 논문에서 구현한 애플리케이션은 집합 기반 POI 검색 알고리즘을 활용하였다. 집합 기반 POI 검색 알고리즘은 오타나 외래어 표기법에 의한 부정확한 질의어를 별도의 데이터베이스 등 외부 자원 없이 알고리즘 차원으로 재구성한다. 집합 기반 POI 검색 알고리즘을 활용할 경우 초성으로 된 스팸 문자열이나, 메시지 내에 숨겨진 스팸 문자열의 검색이 가능하므로 내용이 조작된 스팸 메시지도 판별해낼 수 있다.

본 논문에서 구현한 안티스팸은 자체적으로 구축한 스팸 문자열 데이터베이스를 사용하고 있다. 스팸 메시지 구성 수법과 메시지의 내용이 날로 교묘해짐에 따라 향후 스팸 문자열 데이터베이스의 양을 늘리는 등의 보완이 필요할 것이다. 또한 스팸 메시지의 유형별로 판별해낼 수 있는 알고리즘을 개발하여 다양한 스팸 메시지에 대한 처리를 지원해야 할 것이다.

본 애플리케이션의 구현으로 집합 기반 POI 검색 알고리즘을 POI 문자열뿐만 아니라 스팸 메시지 등으로 확장하여 활용함으로써 집합 기반 검색 알고리즘을 다양한 분야에 응용할 수 있을 것으로 기대된다.

References

[1] Eunbi Go, Jongwoo Lee, JaeWon Lee, An Efficient Set-based POI Search Algorithm, Journal of KIISE: Computing Practices and Letters, vol.19, no.5, pp.242-251, 2013. (in Korean)

[2] Han-Cheol Cho, Geun-sil Jo, Spam-mail Filtering System Using Naive Bayesian Classifier and Message Rule, the Journal of Proceedings of the Korean Information Science Society Conference, vol.29, no.1, pp. 223-225, 2002. (in Korean)

[3] Nam-Cheol Jung, A Method to Block Spam Mail Automatically Through the Connection to Link URL, the Journal of Digital Contents Society, vol.8, no.4, pp. 451-4578, 2007. (in Korean)

[4] Jeungmin Lee, Daehyung Kang, Han-Saem Park, Kyunglag kwon, In-Jeong Chung, A study on the filtering of mobile spam message using collective intelligence, the Journal of Korean Institute of Communications and Information Sciences, pp. 805-806, 2015. (in Korean)

[5] Hyeyeong Ahn, Jongwoo Lee, Design and Implementation of Navigation Operating System APIs for Set-based POI Search Algorithm, Journal of KIISE: Co

mputing Practices and Letters, vol.21, no.3 pp.269-274, 2015. (In Korean)

[6] Android Developers, http://developer.android.com/ndk

[7] Cygwin, http://cygwin.com/index.html

안 혜 영

2013년 : 숙명여자대학교 멀티미디어과학(학사)
2015년 : 숙명여자대학교 대학원 (석사과정)
관심분야 : 운영체제, 검색 시스템, 알고리즘 등

조 완 지

2011~현재: 숙명여자대학교 멀티미디어과학 학사
관심분야 : 모바일 소프트웨어

이 종 우

1990년 : 서울대학교 컴퓨터공학과 (학사)
1992년 : 서울대학교 컴퓨터공학과 (석사)
1996년 : 서울대학교 컴퓨터공학과 (박사)
1996년~1998년: 현대전자㈜ 정보시스템사업본부 과장
1999년~1999년: 현대정보기술㈜ 책임연구원
1999년~2002년: 한림대학교 정보통신공학부 조교수
2002년~2003년: 광운대학교 컴퓨터공학부 조교수
2003년~2004년: 아이닉스소프트㈜ 개발이사
2004년~현재: 숙명여자대학교 멀티미디어과학과 교수
2008년 뉴욕주립대 스토니브룩 Research Scholar
2014년~현재: 한국정보과학회 컴퓨팅의실제 논문지 편집위원장
관심분야 : Mobile System Software, Storage Systems, Computational Finance, Cluster Computing, Parallel and Distributed Operating Systems, and Embedded System Software