(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2015년04월08일
(11) 등록번호 10-1508258
(24) 등록일자 2015년03월27일

(51) 국제특허분류(Int. Cl.)
H04N 1/32 (2006.01)
(21) 출원번호 10-2013-0080263
(22) 출원일자 2013년07월09일
심사청구일자 2013년07월09일
(56) 선행기술조사문헌
JP2008135926 A*
KR1020040011121 A*
KR1020060049165 A*
KR1020100051187 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
성균관대학교산학협력단
경기도 수원시 장안구 서부로 2066, 성균관대학교 내 (천천동)
(72) 발명자
이지형
서울특별시 용산구 청파동2가 26-401
김재광
경기 구리시 인창2로77번길 13, (인창동)
김형식
경기도 수원시 장안구 천천동 천천푸르지오아파트
(74) 대리인
에스앤아이피특허법인

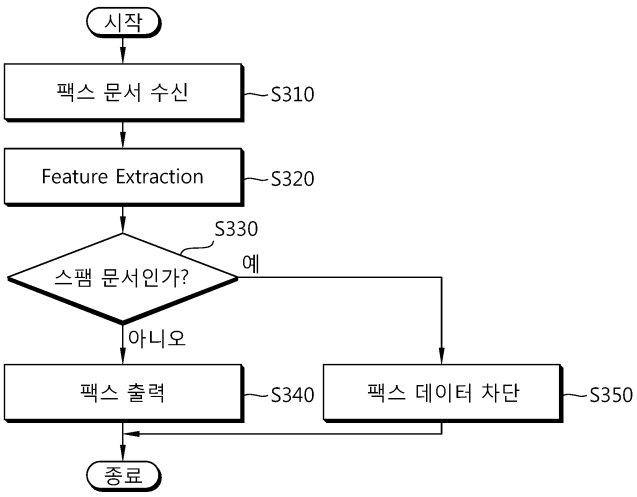
전체 청구항 수 : 총 20 항 심사관 : 한충희

(54) 발명의 명칭 **팩스 스팸 차단 장치, 방법 및 시스템**

(57) 요 약

본 발명의 팩스 스팸 문서 차단 방법은 분석용 팩스 스팸 문서 집단과 분석용 팩스 일반 문서 집단 중 적어도 어느 하나를 토대로 스팸 분류 알고리즘을 생성하는 단계, 상기 스팸 분류 알고리즘을 이용하여 수신된 대상 팩스 문서가 스팸 문서인지 판별하는 판별 단계 및 판별 결과를 기반으로 상기 대상 팩스 문서의 출력 여부를 결정하는 출력 단계를 포함한다. 따라서, 팩스 스팸 시스템을 구현할 때에 불필요한 자원의 소모를 줄일 수 있고, 사용자의 업무 효율을 증가시키므로 생산성의 증가시킨다.

대 표 도 - 도3



이 발명을 지원한 국가연구개발사업
과제고유번호 1345188426
부처명 교육과학기술부
연구관리전문기관 한국연구재단
연구사업명 일반연구자지원
연구과제명 사용자 중심적 마이크로블로그/SNS 정보 가공 및 제공에 관한 연구
기 여 율 1/2
주관기관 성균관대학교(자연과학캠퍼스)
연구기간 2012.05.01 ~ 2013.04.30
이 발명을 지원한 국가연구개발사업
과제고유번호 1415125094
부처명 지식경제부
연구관리전문기관 한국산업기술평가관리원
연구사업명 SW컴퓨팅산업원천기술개발
연구과제명 스마트TV 2.0 소프트웨어 플랫폼
기 여 율 1/2
주관기관 성균관대학교 산학협력단
연구기간 2012.12.01 ~ 2013.11.30

명 세 서

청구범위

청구항 1

분석용 팩스 스팸 문서 집단과 분석용 팩스 일반 문서 집단 중 적어도 어느 하나를 토대로 스팸 분류 알고리즘을 생성하는 단계;

상기 스팸 분류 알고리즘을 이용하여 수신된 대상 팩스 문서가 스팸 문서인지 판별하는 판별 단계; 및

판별 결과를 기반으로 상기 대상 팩스 문서의 출력 여부를 결정하는 출력 단계를 포함하고,

판별이 완료된 문서를 판별 결과에 따라 상기 분석용 팩스 스팸 문서 집단과 상기 분석용 팩스 일반 문서 집단 중 어느 하나에 포함시켜 스팸 분류 알고리즘을 자동 업데이트시키는 단계를 더 포함하는 것을 특징으로 하는 팩스 스팸 문서 차단 방법.

청구항 2

제 1 항에 있어서,

상기 분석용 팩스 스팸 문서는 팩스 문서의 내용을 기반으로 스팸 문서로 판별된 문서이고, 분석용 팩스 일반 문서는 팩스 문서의 내용을 기반으로 하여 수신에 적합한 것으로 판별된 문서인 것을 특징으로 하는 팩스 스팸 문서 차단 방법.

청구항 3

제 2 항에 있어서, 상기 분류 알고리즘 생성 단계는

상기 팩스 스팸 문서 집단 및 상기 팩스 일반 문서 집단을 개별적으로 스캔하는 단계;

상기 스캐닝된 팩스 스팸 문서 집단 및 상기 스캐닝된 팩스 일반 문서 집단에 포함된 단어의 출현 빈도를 개별적으로 산출하는 단계;

상기 출현 빈도를 기반으로 팩스 스팸 문서 모델링 및 팩스 일반 문서 모델링을 개별적으로 수행하는 단계; 및

상기 모델링된 팩스 스팸 문서 및 상기 모델링된 팩스 일반 문서 중 적어도 어느 하나를 기반으로 상기 분류 알고리즘을 생성하는 단계를 포함하는 것을 특징으로 하는 팩스 스팸 문서 차단 방법.

청구항 4

제 3 항에 있어서, 상기 출현 빈도 산출 단계는

상기 스캔된 문서를 전처리하여 불용어를 제거하고 단어만 추출하는 단계; 및

상기 추출된 단어를 기반으로 출현 빈도를 산출하는 단계를 포함하는 것을 특징으로 하는 팩스 스팸 문서 차단 방법.

청구항 5

제 3 항에 있어서, 상기 모델링 수행 단계는

상기 출현 빈도를 기반으로 하여 특징을 선택하는 단계;

상기 선택된 특징을 지지 벡터 머신(SVM: Support Vector Machine)의 특징 벡터로 사용하여 팩스 스팸 문서 모

델링 및 팩스 일반 문서 모델링을 수행하는 단계를 포함하는 것을 특징으로 하는 팩스 스팸 문서 차단 방법.

청구항 6

제 5 항에 있어서, 상기 특징을 선택하는 단계는

상기 출현 빈도가 높은 상위 N 개 - 여기서, N은 임의의 자연수 - 의 단어를 추출하는 단계를 포함하는 것을 특징으로 하는 팩스 스팸 문서 차단 방법.

청구항 7

제 1 항에 있어서,

상기 스팸 분류 알고리즘이 나이브 베이지안 분류 방법(Naive Bayesian Classifier)을 이용하여 생성되는 것을 특징으로 하는 팩스 스팸 문서 차단 방법.

청구항 8

제 1 항에 있어서, 상기 출력 여부 결정 단계는

상기 대상 팩스 문서가 스팸 문서로 판별된 경우에는 출력하지 않고, 지정된 온라인 지점으로 자동으로 전송하는 것을 특징으로 하는 팩스 스팸 문서 차단 방법.

청구항 9

제 8 항에 있어서,

상기 온라인 지점은 사용자 이메일 주소 또는 사용자 지정 웹하드인 것을 특징으로 하는 팩스 스팸 문서 차단 방법.

청구항 10

제 1 항에 있어서,

판별이 완료된 대상 팩스 문서는 판별 결과에 따라 상기 분석용 팩스 스팸 문서 집단과 상기 분석용 팩스 일반 문서 집단 중 어느 하나에 포함되는 것을 특징을 하는 팩스 스팸 문서 차단 방법.

청구항 11

분석용 팩스 스팸 문서 집단과 분석용 팩스 일반 문서 집단 중 적어도 어느 하나를 토대로 스팸 분류 알고리즘을 생성하는 분류 알고리즘 생성부;

상기 스팸 분류 알고리즘을 이용하여 수신된 대상 팩스 문서가 스팸 문서인지 판별하는 판별부; 및

판별 결과를 기반으로 상기 대상 팩스 문서의 출력 여부를 결정하는 출력 결정부를 포함하되,

판별이 완료된 문서를 판별 결과에 따라 상기 분석용 팩스 스팸 문서 집단과 상기 분석용 팩스 일반 문서 집단 중 어느 하나에 포함시켜 스팸 분류 알고리즘을 자동 업데이트시키는 것을 특징으로 하는 팩스 스팸 문서 차단 장치.

청구항 12

제 11 항에 있어서,

상기 분석용 팩스 스팸 문서는 팩스 문서의 내용을 기반으로 스팸 문서로 판별된 문서이고, 분석용 팩스 일반 문서는 팩스 문서의 내용을 기반으로 하여 수신에 적합한 것으로 판별된 문서인 것을 특징으로 하는 팩스 스팸 문서 차단 장치.

청구항 13

제 11 항에 있어서, 상기 분류 알고리즘 생성부는

상기 팩스 스팸 문서 집단 및 상기 팩스 일반 문서 집단을 개별적으로 스캔하는 스캔 수행부;

상기 스캔된 팩스 스팸 문서 집단 및 상기 팩스 일반 문서 집단에 포함된 단어의 출현 빈도를 개별적으로 산출하는 출현 빈도 산출부;

상기 출현 빈도를 기반으로 팩스 스팸 문서 모델링 및 팩스 일반 문서 모델링을 개별적으로 수행하는 모델링부; 및

상기 모델링된 팩스 스팸 문서 및 상기 모델링된 팩스 일반 문서 중 적어도 어느 하나를 기반으로 상기 분류 알고리즘을 생성하는 알고리즘 생성부를 포함하는 것을 특징으로 하는 팩스 스팸 문서 차단 장치.

청구항 14

제 13 항에 있어서, 상기 출현 빈도 산출부는

상기 스캔된 문서를 전처리하여 불용어를 제거하고 단어만 추출하는 단어 추출부; 및

상기 추출된 단어를 기반으로 출현 빈도를 산출하는 산출부를 포함하는 것을 특징으로 하는 팩스 스팸 문서 차단 장치.

청구항 15

제 13 항에 있어서, 상기 모델링부는

상기 출현 빈도가 높은 상위 N 개 - 여기서, N은 임의의 자연수 - 의 단어를 추출하는 상위 단어 추출부; 및

상기 추출된 단어를 지지 벡터 머신(SVM: Support Vector Machine)의 특징 벡터로 사용하여 팩스 스팸 문서 모델링 및 팩스 일반 문서 모델링을 수행하는 펙스 문서 모델링부를 포함하는 것을 특징으로 하는 팩스 스팸 문서 차단 장치.

청구항 16

제 11 항에 있어서,

상기 스팸 분류 알고리즘이 나이브 베이지안 분류 방법(Naive Bayesian Classifier)을 이용하여 생성되는 것을 특징으로 하는 팩스 스팸 문서 차단 장치.

청구항 17

제 11 항에 있어서, 상기 출력 결정부는

상기 대상 팩스 문서가 스팸 문서로 판별된 경우에는 출력하지 않고, 지정된 온라인 지점으로 자동으로 전송하는 것을 특징으로 하는 팩스 스팸 문서 차단 장치.

청구항 18

제 17 항에 있어서,

상기 온라인 지점은 사용자 이메일 주소 또는 사용자 지정 웹하드인 것을 특징으로 하는 팩스 스팸 문서 차단 장치.

청구항 19

제 11 항에 있어서,

판별이 완료된 대상 팩스 문서는 판별 결과에 따라 상기 분석용 팩스 스팸 문서 집단과 상기 분석용 팩스 일반 문서 집단 중 어느 하나에 포함되는 것을 특징을 하는 팩스 스팸 문서 차단 장치.

청구항 20

대상 팩스 문서를 전송하는 수신 팩스 장치로 전송 팩스 장치; 및

분석용 팩스 스팸 문서 집단과 분석용 팩스 일반 문서 집단 중 적어도 어느 하나를 토대로 스팸 분류 알고리즘을 생성하고, 상기 스팸 분류 알고리즘을 이용하여 상기 전송 팩스 장치로부터 수신된 대상 팩스 문서가 스팸 문서인지 판별하며, 판별 결과를 기반으로 상기 대상 팩스 문서의 출력 여부를 결정하는 수신 팩스 장치를 포함하되, 상기 수신 팩스 장치는

판별이 완료된 문서를 판별 결과에 따라 상기 분석용 팩스 스팸 문서 집단과 상기 분석용 팩스 일반 문서 집단 중 어느 하나에 포함시켜 스팸 분류 알고리즘을 자동 업데이트시키는 것을 특징으로 하는 팩스 스팸 문서 차단 시스템.

발명의 설명

기 술 분 야

[0001] 본 발명은 팩스 스팸 차단 알고리즘에 관한 것으로,보다 상세하게는 수신되는 팩스 스팸을 지능적으로 필터링하기 위한 방법에 관한 것이다.

배 경 기 술

[0002] 종래의 팩스 수신 차단을 위한 방법들은 사용자가 직접 스팸 팩스를 송신하는 주체의 전화번호를 직접 등록/삭제/수정 등의 관리를 통해 이루어졌다. 즉, 단순히 송신 전화번호를 등록하여 등록된 스팸 전화번호에서 문서가 전송되는 경우 차단하는 방법을 사용하였다. 이와 같은 경우, 등록, 삭제 등을 수행해야 하는 불편함이 존재하고, 문서의 내용과 상관없이 등록된 전화번호에서 송신되는 모든 무서를 차단하므로 전화번호의 주기적인 업데이터가 필요하며, 반대로 팩스 스팸을 보내는 사람이 다양한 전화번호로 스팸을 송신하는 경우 매번 전화번호를 등록해야 하고, 최소 한번은 스팸을 받아야 하는 문제점이 존재한다.

[0003] 도 1은 종래 팩스 스팸 차단 방법을 개략적으로 나타낸 흐름도이다.

[0004] 도 1을 참조하면, 종래 팩스 스팸 차단 장치는 팩스 문서를 수신한다(S110). 그리고는 수신된 팩스 문서를 전송한 전화 번호가 기존에 등록된 스팩 전화 번호인가 판단한다(S120). 판단 결과, 스팸 전화 번호로부터 수신된 문서이면 팩스 데이터를 차단한다(S130). 반대로 스팸 전화 번호가 아닌 곳으로부터 수신된 문서이면, 일반 문서라고 판단하여 팩스 문서를 출력한다(S140).

[0005] 또한, 블랙 리스트 및 화이트 리스트를 사용하여 스팸 문서를 차단하는 방법이 있을 수 있는데, 이러한 방법은 미리 알려진 리스트를 피해가는 식의 회피 방법에 취약하다는 한계가 있다. 즉, 금지 키워드를 사용하여 스팸을 탐지하면, 공격자는 쉽게 금지 키워드 대산 다른 키워드를 사용하여 탐지 시스템을 우회할 수 있다.

발명의 내용

해결하려는 과제

[0006] 상술한 문제점을 해결하기 위한 본 발명의 목적은 팩스 스팸 차단을 위해, 수신된 팩스의 정보를 분석하여 지능형/자동형 팩스 스팸 알고리즘을 생성하고, 이를 이용하여 효과적인 팩스 스팸 차단을 하는 팩스 스팸 차단 장치, 방법 및 시스템을 제공하는 것이다.

[0007] 이를 통해 불필요한 팩스 스팸의 수신으로 인한 자원의 낭비를 방지하고 업무의 효율성을 증가시킬 수 있다.

과제의 해결 수단

[0008] 상기한 목적을 달성하기 위한 본 발명의 팩스 스팸 문서 차단 방법은 분석용 팩스 스팸 문서 집단과 분석용 팩스 일반 문서 집단 중 적어도 어느 하나를 토대로 스팸 분류 알고리즘을 생성하는 단계, 상기 스팸 분류 알고리즘을 이용하여 수신된 대상 팩스 문서가 스팸 문서인지 판별하는 판별 단계 및 판별 결과를 기반으로 상기 대상 팩스 문서의 출력 여부를 결정하는 출력 단계를 포함할 수 있다.

[0009] 상기 분석용 팩스 스팸 문서는 팩스 문서의 내용을 기반으로 스팸 문서로 판별된 문서이고, 분석용 팩스 일반 문서는 팩스 문서의 내용을 기반으로 하여 수신에 적합한 것으로 판별된 문서일 수 있다.

[0010] 상기 분류 알고리즘 생성 단계는 상기 팩스 스팸 문서 집단 및 상기 팩스 일반 문서 집단을 개별적으로 스캔하는 단계, 상기 스캐닝된 팩스 스팸 문서 집단 및 상기 스캐닝된 팩스 일반 문서 집단에 포함된 단어의 출현 빈도를 개별적으로 산출하는 단계, 상기 출현 빈도를 기반으로 팩스 스팸 문서 모델링 및 팩스 일반 문서 모델링을 개별적으로 수행하는 단계 및 상기 모델링된 팩스 스팸 문서 및 상기 모델링된 팩스 일반 문서 중 적어도 어느 하나를 기반으로 상기 분류 알고리즘을 생성하는 단계를 포함할 수 있다.

[0011] 상기 출현 빈도 산출 단계는 상기 스캔된 문서를 전처리하여 불용어를 제거하고 단어만 추출하는 단계 및 상기 추출된 단어를 기반으로 출현 빈도를 산출하는 단계를 포함할 수 있다.

[0012] 상기 모델링 수행 단계는 상기 출현 빈도를 기반으로 하여 특징을 선택하는 단계 및 상기 선택된 특징을 지지 벡터 머신(SVM: Support Vector Machine)의 특징 벡터로 사용하여 팩스 스팸 문서 모델링 및 팩스 일반 문서 모델링을 수행하는 단계를 포함할 수 있다.

[0013] 상기 특징을 선택하는 단계는 상기 출현 빈도가 높은 상위 N 개 - 여기서, N은 임의의 자연수 - 의 단어를 추출하는 단계를 포함할 수 있다.

[0014] 상기 스팸 분류 알고리즘이 나이브 베이지안 분류 방법(Naive Bayesian Classifier)을 이용하여 생성될 수 있다.

[0015] 상기 출력 여부 결정 단계는 상기 대상 팩스 문서가 스팸 문서로 판별된 경우에는 출력하지 않고, 지정된 온라인 지점으로 자동으로 전송할 수 있다.

[0016] 상기 온라인 지점은 사용자 이메일 주소 또는 사용자 지정 웹하드일 수 있다.

[0017] 판별이 완료된 대상 팩스 문서는 판별 결과에 따라 상기 분석용 팩스 스팸 문서 집단과 상기 분석용 팩스 일반 문서 집단 중 어느 하나에 포함될 수 있다.

[0018] 상기한 목적을 달성하기 위한 본 발명의 팩스 스팸 문서 차단 장치는 분석용 팩스 스팸 문서 집단과 분석용 팩스 일반 문서 집단 중 적어도 어느 하나를 토대로 스팸 분류 알고리즘을 생성하는 분류 알고리즘 생성부, 상기 스팸 분류 알고리즘을 이용하여 수신된 대상 팩스 문서가 스팸 문서인지 판별하는 판별부 및 판별 결과를 기반으로 상기 대상 팩스 문서의 출력 여부를 결정하는 출력 결정부를 포함할 수 있다.

[0019] 상기 분석용 팩스 스팸 문서는 팩스 문서의 내용을 기반으로 스팸 문서로 판별된 문서이고, 분석용 팩스 일반 문서는 팩스 문서의 내용을 기반으로 하여 수신에 적합한 것으로 판별된 문서일 수 있다.

[0020] 상기 분류 알고리즘 생성부는 상기 팩스 스팸 문서 집단 및 상기 팩스 일반 문서 집단을 개별적으로 스캔하는 스캔 수행부, 상기 스캔된 팩스 스팸 문서 집단 및 상기 팩스 일반 문서 집단에 포함된 단어의 출현 빈도를 개

별적으로 산출하는 출현 빈도 산출부, 상기 출현 빈도를 기반으로 팩스 스팸 문서 모델링 및 팩스 일반 문서 모델링을 개별적으로 수행하는 모델링부 및 상기 모델링된 팩스 스팸 문서 및 상기 모델링된 팩스 일반 문서 중 적어도 어느 하나를 기반으로 상기 분류 알고리즘을 생성하는 알고리즘 생성부를 포함할 수 있다.

[0021] 상기 출현 빈도 산출부는 상기 스캔된 문서를 전처리하여 불용어를 제거하고 단어만 추출하는 단어 추출부 및 상기 추출된 단어를 기반으로 출현 빈도를 산출하는 산출부를 포함할 수 있다.

[0022] 상기 모델링부는 상기 출현 빈도가 높은 상위 N 개 - 여기서, N은 임의의 자연수 - 의 단어를 추출하는 상위 단어 추출부 및 상기 추출된 단어를 지지 벡터 머신(SVM: Support Vector Machine)의 특징 벡터로 사용하여 팩스 스팸 문서 모델링 및 팩스 일반 문서 모델링을 수행하는 팩스 문서 모델링부를 포함할 수 있다.

[0023] 상기 스팸 분류 알고리즘이 나이브 베이지안 분류 방법(Naive Bayesian Classifier)을 이용하여 생성될 수 있다.

[0024] 상기 출력 결정부는 상기 대상 팩스 문서가 스팸 문서로 판별된 경우에는 출력하지 않고, 지정된 온라인 지점으로 자동으로 전송할 수 있다.

[0025] 상기 온라인 지점은 사용자 이메일 주소 또는 사용자 지정 웹하드일 수 있다.

[0026] 판별이 완료된 대상 팩스 문서는 판별 결과에 따라 상기 분석용 팩스 스팸 문서 집단과 상기 분석용 팩스 일반 문서 집단 중 어느 하나에 포함될 수 있다.

[0027] 상기한 목적을 달성하기 위한 본 발명의 팩스 스팸 문서 차단 시스템은 대상 팩스 문서를 전송하는 수신 팩스 장치로 전송 팩스 장치 및 분석용 팩스 스팸 문서 집단과 분석용 팩스 일반 문서 집단 중 적어도 어느 하나를 토대로 스팸 분류 알고리즘을 생성하고, 상기 스팸 분류 알고리즘을 이용하여 상기 전송 팩스 장치로부터 수신된 대상 팩스 문서가 스팸 문서인지 판별하며, 판별 결과를 기반으로 상기 대상 팩스 문서의 출력 여부를 결정하는 수신 팩스 장치를 포함할 수 있다.

발명의 효과

[0028] 본 발명의 팩스 스팸 차단 장치, 방법 및 시스템에 따르면, 팩스 스팸 시스템을 구현할 때에 불필요한 자원의 소모를 줄일 수 있고, 사용자의 업무 효율을 증가시키므로 생산성의 증가를 도모하는 효과가 있다.

[0029] 또한, 본 발명의 팩스 스팸 차단 장치, 방법 및 시스템에 따르면, 분류기의 생성과 업데이트로 스팸 차단의 높은 정확도를 유지하고 유지 보수 비용을 최소화하는 효과가 있다.

도면의 간단한 설명

[0030] 도 1은 종래 팩스 스팸 차단 방법을 개략적으로 나타낸 흐름도,

도 2는 본 발명의 일 실시예에 따른 팩스 스팸 차단 방법이 적용될 수 있는 시스템을 개략적으로 나타낸 도면,

도 3은 본 발명의 일 실시예에 따른 팩스 스팸 차단 방법을 개략적으로 나타낸 흐름도,

도 4는 본 발명의 일 실시예에 따른 팩스 스팸 차단 방법의 특징 추출 단계를 구체적으로 나타낸 상세흐름도,

도 5는 본 발명의 일 실시예에 따른 팩스 스팸 차단 방법의 출력 여부 결정 단계를 구체적으로 나타낸 상세흐름도,

도 6은 본 발명의 일 실시예에 따른 팩스 스팸 차단 방법에 따라 스팸 문서로 결정된 경우의 처리를 설명하기 위한 도면,

도 7은 본 발명의 일 실시예에 따른 팩스 스팸 차단 장치를 개략적으로 나타낸 블록도,

도 8은 본 발명의 일 실시예에 따른 팩스 스팸 차단 장치의 분류 알고리즘 생성부를 구체적으로 나타낸 상세블록도,

도 9는 본 발명의 일 실시예에 따른 팩스 스팸 차단 장치의 출현 빈도 산출부를 구체적으로 나타낸 상세블록도,

도 10은 본 발명의 일 실시예에 따른 팩스 스팸 차단 장치의 모델링부를 구체적으로 나타낸 상세블록도,

도 11은 본 발명의 일 실시예에 따른 팩스 스팸 차단 방법의 성능을 실험하기 위해 사용하는 confusion matrix를 나타낸 도면,

도 12a는 본 발명의 일 실시예에 따른 팩스 스팸 차단 방법의 세 가지 분류 방식의 ACC 결과를 나타낸 표,

도 12b는 본 발명의 일 실시예에 따른 팩스 스팸 차단 방법의 세 가지 분류 방식의 Pre_spam 결과를 나타낸 표,

도 12c는 본 발명의 일 실시예에 따른 팩스 스팸 차단 방법의 세 가지 분류 방식의 Rec_spam 결과를 나타낸 표,

도 12d는 본 발명의 일 실시예에 따른 팩스 스팸 차단 방법의 세 가지 분류 방식의 Rec_norm 결과를 나타낸 표,

도 13은 고급 스팸 공격에서의 본 발명의 일 실시예에 따른 팩스 스팸 차단 방법의 세 가지 분류 방식의 F-measure를 비교한 그래프이다.

발명을 실시하기 위한 구체적인 내용

[0031] 본 발명은 다양한 변경을 가할 수 있고 여러 가지 실시예를 가질 수 있는 바, 특정 실시예들을 도면에 예시하고 상세하게 설명하고자 한다.

[0032] 그러나, 이는 본 발명을 특정한 실시 형태에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다.

[0033] 제 1, 제 2 등의 용어는 다양한 구성요소들을 설명하는데 사용될 수 있지만, 상기 구성요소들은 상기 용어들에 의해 한정되어서는 안 된다. 상기 용어들은 하나의 구성요소를 다른 구성요소로부터 구별하는 목적으로만 사용된다. 예를 들어, 본 발명의 권리 범위를 벗어나지 않으면서 제 1 구성요소는 제 2 구성요소로 명명될 수 있고, 유사하게 제 2 구성요소도 제 1 구성요소로 명명될 수 있다. 및/또는 이라는 용어는 복수의 관련된 기재된 항목들의 조합 또는 복수의 관련된 기재된 항목들 중의 어느 항목을 포함한다.

[0034] 어떤 구성요소가 다른 구성요소에 "연결되어" 있다거나 "접속되어" 있다고 언급된 때에는, 그 다른 구성요소에 직접적으로 연결되어 있거나 또는 접속되어 있을 수도 있지만, 중간에 다른 구성요소가 존재할 수도 있다고 이해되어야 할 것이다. 반면에, 어떤 구성요소가 다른 구성요소에 "직접 연결되어" 있다거나 "직접 접속되어" 있다고 언급된 때에는, 중간에 다른 구성요소가 존재하지 않는 것으로 이해되어야 할 것이다.

[0035] 본 출원에서 사용한 용어는 단지 특정한 실시예를 설명하기 위해 사용된 것으로, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 출원에서, "포함하다" 또는 "가지다" 등의 용어는 명세서상에 기재된 특징, 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.

[0036] 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미를 가지고 있다. 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥상 가지는 의미와 일치하는 의미를 가진 것으로 해석되어야 하며, 본 출원에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.

[0037] 이하, 첨부한 도면들을 참조하여, 본 발명의 바람직한 실시예를 보다 상세하게 설명하고자 한다. 본 발명을 설명함에 있어 전체적인 이해를 용이하게 하기 위하여 도면상의 동일한 구성요소에 대해서는 동일한 참조부호를 사용하고 동일한 구성요소에 대해서 중복된 설명은 생략한다.

[0038] 팩스 스팸 차단 시스템

[0039] 도 2는 본 발명의 일 실시예에 따른 팩스 스팸 차단 방법이 적용될 수 있는 시스템을 개략적으로 나타낸 도면이다. 도 2에 도시된 바와 같이, 본 발명의 일 실시예에 따른 팩스 스팸 차단 시스템은 전송 팩스 장치(10-1, 10-2, ..., 10-N) 및 수신 팩스 장치(20)를 포함할 수 있다.

[0040] 도 2를 참조하면, 전송 팩스 장치(10-1, 10-2, ..., 10-N)는 수신 팩스 장치(20)로 팩스 문서를 전송한다. 전송 팩스 장치(10-1, 10-2, ..., 10-N)는 무선 또는 유선 네트워크를 통해 수신 팩스 장치(20)로 팩스 문서를 전송할 수 있다. 전송 팩스 장치(10-1, 10-2, ..., 10-N)는 원하지 않는 광고 정보를 포함하는 스팸 문서 또는 일반 문서를 전송할 수 있다. 여기서, 일반 문서는 팩스 문서의 내용을 기반으로 사용자가 수신하길 원하는 문서일 수 있다.

[0041] 수신 팩스 장치(20)는 무선 또는 유선 네트워크를 통해 팩스 문서를 수신한다. 수신 팩스 장치(20)는 팩스 스팸 문서와 팩스 일반 문서 중 적어도 어느 하나를 토대로 스팸 분류 알고리즘을 생성할 수 있다. 그리고는, 생성된 스팸 분류 알고리즘을 이용하여 전송 팩스 장치(10-1, 10-2, ..., 10-N)로부터 수신된 팩스 문서가 스팸 문서인지 판별할 수 있다. 수신 팩스 장치(20)는 판별 결과를 기반으로 수신된 팩스 문서의 출력 여부를 결정할 수 있다. 수신 팩스 문서가 일반 문서이면 문서를 출력하고, 그렇지 않으면, 출력을 하지 않고 사용자가 지정한 온라인 지점으로 상기 팩스 문서를 전송할 수 있다.

[0042] 팩스 스팸 차단 방법

[0043] 도 3은 본 발명의 일 실시예에 따른 팩스 스팸 차단 방법을 개략적으로 나타낸 흐름도이다.

[0044] 도 3을 참조하면, 본 발명의 일 실시예에 따른 팩스 스팸 차단 장치는 먼저 팩스 문서를 수신한다(S310).

[0045] 그리고는 특징 추출(Feature Extraction)을 수행한다(S320). 특징 추출은 변환과 적절한 결합을 기반으로 새로운 특징들을 만들어 내는 것이다. 상기 특징 추출은 팩스 스팸 문서 집단과 팩스 일반 문서 집단으로부터 특징을 추출하여 스팸 분류 알고리즘을 생성함으로써 이루어질 수 있다. 여기서, 팩스 스팸 문서 집단 및 팩스 일반 문서 집단은 스팸 분류 알고리즘을 생성하기 위한 분석용 모집단이다. 이를 위해, 사용자의 정의에 따른 팩스 스팸 문서와 팩스 일반 문서를 이용하여 분류기 학습을 수행해야 한다. 팩스 스팸 문서는 단순히 특정 주제 관련 팩스이거나 특정 전화번호에서 송신된 팩스가 아니라 팩스 문서 내용에 따라 사용자가 원하지 않는 팩스 문서로서 사용자가 학습에 사용할 문서로 정의할 수 있다. 팩스 일반 문서는 전술한 바와 같이, 팩스 문서의 내용을 기반으로 하여 사용자가 수신하기 원하는 문서로 정의할 수 있다.

[0046] 특징 추출을 완료하면, 스팸 문서 차단 장치는 수신된 팩스 문서가 스팸 문서인지 판단한다(S330). 특징 추출 단계(S320)에서 생성된 분류 알고리즘을 이용하여 수신된 팩스 문서가 스팸 문서인지 판단한다.

[0047] 판단 결과, 스팸 문서가 아닌 경우, 사용자가 원하는 일반 문서로 판단하여 팩스 문서를 출력한다(S340). 반대로, 스팸 문서인 경우, 팩스 데이터를 차단한다(S350).

[0048] 도 4는 본 발명의 일 실시예에 따른 팩스 스팸 차단 방법의 특징 추출 단계를 구체적으로 나타낸 상세흐름도이다.

[0049] 도 4를 참조하면, 전체적으로 팩스 스팸 차단 장치는 대상 팩스 문서를 입력 받고(S410), 스팸 문서인지 판별하기 위한 스팸 분류 알고리즘을 생성한 후(S430), 대상 팩스 문서의 스팸 여부를 판별한다(S450). 여기서, 스팸 분류 알고리즘을 생성하는 단계(S430)가 핵심이 될 수 있는데, 이를 자세히 살펴보면 다음과 같다.

[0050] 본 발명의 일 실시예에 따르면, 스팸 문서 차단 장치는 팩스 스팸 문서 모델과 팩스 일반 문서 모델 중 적어도 어느 하나를 통해 스팸 분류 알고리즘을 생성한다. 따라서, 두 가지 모델을 개별적으로 생성할 수 있다. 즉, 사용자 설정에 따라 팩스 스팸 문서 모델만을 이용할지, 팩스 일반 문서 모델만을 이용할지, 아니면 둘 모두를 이용할지를 선택할 수 있고, 이에 따라 모델링 프로세스가 진행될 수 있다.

[0051] 이를 위해, 스팸 문서 차단 장치는 팩스 스팸 문서 및/또는 팩스 일반 문서를 OCR(Optical Character Reader) 스캔한다(S431, S441). 즉, 이미지를 스캔하여 기계에서 읽을 수 있는 포맷으로 변환한다. OCR 스캐닝 기술은 현재 공지되어 있는 복수의 기술을 포함할 수 있다.

[0052] 다음, 스팸 문서 차단 장치는 스캐닝된 문서를 전처리하여 단어만 추출한다(S433, S443). 스캐닝된 문서에는 특별한 의미를 지닌 단어가 아닌 불용어를 다수 포함하고 있으므로, 이를 제거하여 단어만을 추출한다. 스팸 문서 차단 장치는 불용어 사전을 이용하여 전처리를 수행할 수 있다.

[0053] 그리고는, 각 단어의 출현 빈도를 산출한다(S435, S445). 즉, 스팸 문서 차단 장치는 특징 추출을 위해, 팩스

문서 내의 단어의 출현 빈도를 분석할 수 있다.

[0054] 다음으로, 스팸 문서 차단 장치는 지지 벡터 머신(SVM: Support Vector Machine) 또는 나이브 베이지안 분류 방법(Naive Bayesian Classifier)을 구성하기 위해, 팩스 스팸 문서 및/또는 팩스 일반 문서의 두 클래스의 특징을 선택한다(S437, S447). 특징 선택은 특징 추출과는 다른 개념으로, 입력되는 특징 집합 중 최선의 부분 집합을 골라내는 것을 의미한다. 본 발명에서는, 분류기의 특징으로서 각 클래스의 단어 출현 빈도를 선택한다. 이때, 모든 단어의 모든 출현 빈도를 특징으로 이용할 수 있는데, 이는 비효율적일 수 있다. 따라서, 스팸 문서 차단 장치는 문서들의 특징들 중 더 큰 임팩트를 갖는 특징들, 즉 출현 빈도가 높은 단어들을 선택한다. 즉, 이러한 출현 빈도 기반의 특징 선택은 텍스트 마이닝에 폭넓게 사용될 수 있다.

[0055] 본 발명의 다른 실시예에 따르면, 출현 빈도가 높은 N개의 단어를 이용하여 단어가 나타난 정도에 따라 각 집단에 포함될 확률을 높이는 방법으로 분류할 수 있고, 또는, 다른 방법으로 출현 빈도가 높은 N개의 단어를 지지 벡터 머신의 특징 벡터(feature vector)로 사용하여 분류 알고리즘을 생성할 수 있다.

[0056] 마지막으로, 스팸 문서 차단 장치는 두 개의 대표적인 방법(예컨대, 지지 벡터 머신 또는 나이브 베이지안)을 통해 팩스 스팸 문서 모델링 및 팩스 일반 문서 모델링을 수행한다(S439, S449). 여기서, 지지 벡터 머신을 사용하는 경우, 전술한 바와 같이, 출현 빈도가 높은 N개의 단어를 지지 벡터 머신의 특징 벡터로 사용하여 모델링을 수행할 수 있다. 지지 벡터 머신 모델을 생성하는 것은 훈련 단계 및 테스트 단계를 통해 이루어질 수 있다.

[0057] 다른 방법으로, 나이브 베이지안 분류 방법이 사용될 수 있는데, 이는 각 클래스에서 나타난 단어는 그 클래스를 나타내는 특징(feature)이고, 각 단어는 출현한 어떤 문서에 대해 다른 단어들과 연관이 없다는 가정을 기반으로 이산 분리 모델을 생성하는 것이다. 따라서, 출현 빈도가 높은 상기 N 개의 단어를 토대로 모델링을 수행할 수 있다. 나이브 베이지안 분류 방법을 통한 모델링은 실행하기에 단순하고, 문서 모델링이 빠르다는 장점이 있다. 이는 단어 모델의 백(bag)으로써 잘 작동하고, 문서 모델링에 매우 적합하다.

[0058] 이렇게 두 가지 방법 중 어느 하나를 사용하여 팩스 스팸 문서 모델링 및 팩스 일반 문서 모델링을 수행할 수 있고, 상기 두 모델링된 문서 중 적어도 어느 하나를 사용하여 분류 알고리즘을 생성할 수 있다.

[0059] 도 5는 본 발명의 일 실시예에 따른 팩스 스팸 차단 방법의 출력 여부 결정 단계를 구체적으로 나타낸 상세흐름도이다.

[0060] 도 5를 참조하면, 팩스 스팸 차단 장치는 생성된 스팸 분류 알고리즘을 이용하여 수신된 대상 팩스 문서가 스팸 문서인지 판단한다(S510). 그리고는, 판단 결과, 스팸 문서이면 지정된 온라인 지점으로 전송한다(S520). 만약, 스팸 문서가 아니라면 팩스 문서를 출력한다(S530). 이렇게 함으로써, 스팸 문서의 무조건적인 출력을 방지할 수 있어 전력 및 종이 낭비를 줄일 수 있다.

[0061] 도 6은 본 발명의 일 실시예에 따른 팩스 스팸 차단 방법에 따라 스팸 문서로 결정된 경우의 처리를 설명하기 위한 도면이다.

[0062] 도 6을 참조하면, 본 발명의 팩스 스팸 차단 장치는 스팸 문서로 판별되면 사용자가 지정한 온라인 지점으로 전송되어 무조건적인 소실을 방지할 수 있다. 예컨대, 사용자는 사용자 인터페이스를 통해 사용자가 사용하는 이메일(620) 또는 인터넷을 통해 액세스할 수 있는 웹하드(630)로 스팸 문서를 일시 저장하도록 설정할 수 있다. 상기 설정에 따라 팩스 스팸 차단 장치는 스팸 문서로 판별된 수신 팩스 문서를 사용자 이메일 주소(620) 또는 웹하드(630)로 전송한다. 사용자는 본인이 설정한 상기 이메일 주소(620) 또는 웹하드(630)에서 스팸 문서를 확인하고, 스팸이 아닌 경우 다시 복원하여 출력할 수 있는 기회를 확보할 수 있다. 이를 통해 무조건적으로 문서가 스팸 문서로 판별되어 버려지는 것을 방지할 수 있다.

[0063] 이렇게 하나의 수신 팩스 문서에 대한 출력 여부가 결정되고 나면, 상기 수신 팩스 문서도 일반 문서 또는 스팸 문서로의 판별에 따라 분석용 팩스 스팸 문서 집단 또는 분석용 팩스 일반 문서 집단에 포함될 수 있고, 최신 자료가 계속 업데이트되어 종국에는 스팸 분류 알고리즘이 최신으로 업데이트될 수 있다.

[0064] 팩스 스팸 차단 장치

[0065] 도 7은 본 발명의 일 실시예에 따른 팩스 스팸 차단 장치를 개략적으로 나타낸 블록도이다. 도 7에 도시된 바와

같이, 본 발명의 일 실시예에 다른 팩스 차단 장치는 분류 알고리즘 생성부(710), 판별부(720) 및 출력 결정부(730)를 포함할 수 있다.

[0066] 도 7을 참조하면, 분류 알고리즘 생성부(710)는 특징 추출(Feature Extraction)을 수행한다. 분류 알고리즘 생성부(710)는 팩스 스팸 문서 집단과 팩스 일반 문서 집단으로부터 특징을 추출하여 스팸 분류 알고리즘을 생성함으로써 이루어질 수 있다. 여기서, 팩스 스팸 문서 집단 및 팩스 일반 문서 집단은 스팸 분류 알고리즘을 생성하기 위한 분석용 모집단이다. 이를 위해, 사용자의 정의에 따른 팩스 스팸 문서와 팩스 일반 문서를 이용하여 분류기 학습을 수행해야 한다. 팩스 스팸 문서는 단순히 특정 주제 관련 팩스이거나 특정 전화번호에서 송신된 팩스가 아니라 팩스 문서 내용에 따라 사용자가 원하지 않는 팩스 문서로서 사용자가 학습에 사용할 문서로 정의할 수 있다. 팩스 일반 문서는 전술한 바와 같이, 팩스 문서의 내용을 기반으로 하여 사용자가 수신하기 원하는 문서로 정의할 수 있다.

[0067] 판별부(720)는 수신된 팩스 문서가 스팸 문서인지 판단한다. 분류 알고리즘 생성부(710)에서 생성된 분류 알고리즘을 이용하여 수신된 팩스 문서가 스팸 문서인지 판단한다.

[0068] 출력 결정부(730)는 판별부(720)에서의 판단 결과에 따라 수신 팩스 문서의 출력 여부를 결정한다. 판단 결과, 스팸 문서가 아닌 경우, 사용자가 원하는 일반 문서로 판단하여 팩스 문서를 출력한다. 반대로, 스팸 문서인 경우, 팩스 데이터를 차단한다. 이때, 스팸 문서로 판별되어 차단되는 팩스 문서는 바로 제거되는 것이 아니라 지정된 온라인 지점으로 전송될 수 있다. 이렇게 함으로써, 스팸 문서의 무조건적인 출력을 방지할 수 있어 전력 및 종이 낭비를 줄일 수 있다. 사용자는 사용자 인터페이스를 통해 사용자가 사용하는 이메일 또는 인터넷을 통해 액세스할 수 있는 웹하드로 스팸 문서를 일시 저장하도록 설정할 수 있다. 상기 설정에 따라 출력 결정부(730)는 스팸 문서로 판별된 수신 팩스 문서를 사용자 이메일 주소 또는 웹하드로 전송한다. 사용자는 설정된 지점에서 스팸 문서를 확인하고, 스팸이 아닌 경우 다시 복원하여 출력할 수 있는 기회를 확보할 수 있다.

[0069] 이렇게 하나의 수신 팩스 문서에 대한 출력 여부가 결정되고 나면, 상기 수신 팩스 문서도 일반 문서 또는 스팸 문서로의 판별에 따라 분석용 팩스 스팸 문서 집단 또는 분석용 팩스 일반 문서 집단에 포함될 수 있다.

[0070] 도 8은 본 발명의 일 실시예에 따른 팩스 스팸 차단 장치의 분류 알고리즘 생성부(710)를 구체적으로 나타낸 상세블록도이다. 도 8에 도시된 바와 같이, 분류 알고리즘 생성부(710)는 스캔 수행부(810), 출현 빈도 산출부(820), 모델링부(830) 및 알고리즘 생성부(840)를 포함할 수 있다.

[0071] 도 8을 참조하면, 스캔 수행부(810)는 팩스 스팸 문서 모델과 팩스 일반 문서 모델 중 적어도 어느 하나를 통해 스팸 분류 알고리즘을 생성하기 위해, 팩스 스팸 문서 및/또는 팩스 일반 문서를 OCR(Optical Character Reader) 스캔한다. 즉, 이미지를 스캔하여 기계에서 읽을 수 있는 포맷으로 변환한다. OCR 스캐닝 기술은 현재 공지되어 있는 복수의 기술을 포함할 수 있다.

[0072] 출현 빈도 산출부(820)는 특징 추출을 위해, 팩스 스팸 문서 집단 또는 팩스 일반 문서 집단 내의 단어의 출현 빈도를 분석할 수 있다.

[0073] 모델링부(830)는 분석된 출현 빈도를 토대로 특징을 선택하여 팩스 스팸 문서 모델링 및 팩스 일반 문서 모델링을 수행할 수 있다. 이때, 지지 벡터 머신 또는 나이브 베이지안 분류 방법이 사용될 수 있다.

[0074] 알고리즘 생성부(840)는 팩스 스팸 문서 모델과 팩스 일반 문서 모델 중 적어도 어느 하나를 통해 스팸 분류 알고리즘을 생성한다. 알고리즘 생성부(840)는 두 가지 모델을 개별적으로 생성할 수 있다. 즉, 사용자 설정에 따라 팩스 스팸 문서 모델만을 이용할지, 팩스 일반 문서 모델만을 이용할지, 아니면 둘 모두를 이용할지를 선택할 수 있고, 이에 따라 모델링 프로세스가 진행될 수 있다.

[0075] 도 9는 본 발명의 일 실시예에 따른 팩스 스팸 차단 장치의 출현 빈도 산출부(820)를 구체적으로 나타낸 상세블록도이다. 도 9에 도시된 바와 같이, 본 발명의 일 실시예에 따른 출현 빈도 산출부(820)는 단어 추출부(910) 및 산출부(920)를 포함할 수 있다.

[0076] 도 9를 참조하면, 단어 추출부(910)는 스캐닝된 문서를 전처리하여 단어만 추출한다. 스캐닝된 문서에는 특별한 의미를 지닌 단어가 아닌 불용어를 다수 포함하고 있으므로, 이를 제거하여 단어만을 추출한다. 스팸 문서 차단 장치는 불용어 사전을 이용하여 전처리를 수행할 수 있다.

[0077] 산출부(920)는 출현 빈도를 산출한다. 산출부(920)는 특징 추출을 위해, 팩스 문서 내의 단어의 출현 빈도를 분석할 수 있다.

[0078] 도 10은 본 발명의 일 실시예에 따른 팩스 스팸 차단 장치의 모델링부(830)를 구체적으로 나타낸 상세블록도이다. 도 10에 도시된 바와 같이, 모델링부(830)는 특징 선택부(1010) 및 팩스 문서 모델링부(1020)를 포함할 수 있다.

[0079] 특징 선택부(1010)는 지지 벡터 머신(SVM: Support Vector Machine) 또는 나이브 베이지안 분류 방법(Naive Bayesian Classifier)을 구성하기 위해, 팩스 스팸 문서 및/또는 팩스 일반 문서의 두 클래스의 특징을 선택한다. 특징 선택은 특징 추출과는 다른 개념으로, 입력되는 특징 집합 중 최선의 부분 집합을 골라내는 것을 의미한다. 특징 선택부(1010)는 분류기의 특징으로서 각 클래스의 단어 출현 빈도를 선택할 수 있다. 이때, 모든 단어의 모든 출현 빈도를 특징으로 이용할 수 있는데, 이는 비효율적일 수 있다. 따라서, 스팸 문서 차단 장치는 문서들의 특징들 중 더 큰 임팩트를 갖는 특징들, 즉 출현 빈도가 높은 단어들을 선택한다. 즉, 이러한 출현 빈도 기반의 특징 선택은 텍스트 마이닝에 폭넓게 사용될 수 있다.

[0080] 본 발명의 다른 실시예에 따르면, 특징 선택부(1010)는 출현 빈도가 높은 N개의 단어를 이용하여 단어가 나타난 정도에 따라 각 집단에 포함될 확률을 높이는 방법으로 분류할 수 있다. 또는, 특징 선택부(1010)는 출현 빈도가 높은 N개의 단어를 지지 벡터 머신의 특징 벡터(feature vector)로 사용하여 분류 알고리즘을 생성할 수 있다.

[0081] 팩스 문서 모델링부(1020)는 두 개의 대표적인 방법(예컨대, 지지 벡터 머신 또는 나이브 베이지안)을 통해 팩스 스팸 문서 모델링 및 팩스 일반 문서 모델링을 수행한다. 여기서, 지지 벡터 머신을 사용하는 경우, 전술한 바와 같이, 출현 빈도가 높은 N개의 단어를 지지 벡터 머신의 특징 벡터로 사용하여 모델링을 수행할 수 있다. 지지 벡터 머신 모델을 생성하는 것은 훈련 단계 및 테스트 단계를 통해 이루어질 수 있다.

[0082] 다른 방법으로, 팩스 문서 모델링부(1020)는 나이브 베이지안 분류 방법이 사용될 수 있는데, 이는 각 클래스에서 나타난 단어는 그 클래스를 나타내는 특징(feature)이고, 각 단어는 출현한 어떤 문서에 대해 다른 단어들과 연관이 없다는 가정을 기반으로 이산 분리 모델을 생성하는 것이다. 따라서, 팩스 문서 모델링부(1020)는 출현 빈도가 높은 상기 N 개의 단어를 토대로 모델링을 수행할 수 있다. 나이브 베이지안 분류 방법을 통한 모델링은 실행하기에 단순하고, 문서 모델링이 빠르다는 장점이 있다. 이는 단어 모델의 백(bag)으로써 잘 작동하고, 문서 모델링에 매우 적합하다.

[0083] 시뮬레이션 결과

[0084] 본 발명의 팩스 스팸 차단 방법의 성능을 검증하기 위해 시뮬레이션을 수행하였다. 먼저, 팩스 스팸 분류 알고리즘을 생성하기 위해 팩스 스팸 문서와 팩스 일반 문서를 수집하였고, 이때, 수집 문서는 사용자의 주관적인 판단에 의해 다양한 내용으로 분류되어 수집되었다. 각 수집한 팩스 문서를 집단별로 OCR 스캔하여 단어의 집단으로 취합한 후, 전처리를 수행하였다. 이후, 각 단어의 출현 빈도를 파악하여 문서별로 가장 많이 나타난 단어와 그 빈도를 파악하고 이를 이용하여 스팸 문서와 일반 문서의 특징을 선정하였다. 또한, 지지 벡터 머신과 나이브 베이지안 분류 방법을 사용하여 모델링을 수행하였다.

[0085] 도 11은 본 발명의 일 실시예에 따른 팩스 스팸 차단 방법의 성능을 실험하기 위해 사용하는 confusion matrix를 나타낸 도면이다.

[0086] 도 11을 참조하면, 매트릭스를 통해 정확도(ACC), 스팸 검출의 정밀도(precesion), 스팸 검출의 리콜(recall) 및 일반 검출의 리콜을 산출하였다. 이는 다음과 같이 계산될 수 있다.

수학식 1

[0087]

$$ACC = \frac{a+d}{a+b+c+d} \quad (1)$$

$$Pre\_spam = \frac{a}{a+b} \quad (2)$$

$$Rec\_spam = \frac{a}{a+c} \quad (3)$$

$$Rec\_norm = \frac{d}{b+d} \quad (4)$$

[0088] 정확도(ACC)는 본 발명에 따른 팩스 스팸 시스템의 전체 성능을 의미한다. 이는 시스템이 실제 스팸을 스팸이라고, 실제 일반 문서를 일반 문서라고 판별할 때 증가한다.

[0089] 도 12a는 본 발명의 일 실시예에 따른 팩스 스팸 차단 방법의 세 가지 분류 방식의 ACC 결과를 나타낸 표이다.

[0090] 도 12a를 참조하면, RB는 룰 기반 필터링 방법을 통한 모델링을 수행한 경우에 해당하고, SVM은 지지 벡터 머신을 통한 분류 방법을 사용하여 모델링한 경우를 나타내며, NB는 나이브 베이지안 방법을 사용한 경우를 나타낸다. 도 12a에 도시된 바와 같이, 룰 기반 필터링 방법의 정확도가 55.35%로 가장 낮고, 본 발명의 실시예에 따른 팩스 차단 시스템이 사용하는 SVM 및 NB는 거의 동일한 결과로 91% 대의 높은 정확도를 나타낸다. 테이블 상단의 10, 20,...100의 숫자는 선택된 특징들의 수를 나타낸다.

[0091] 다시 도 11로 돌아가서, Pre_spam은 시스템이 얼마나 스팸을 잘 검출하는지를 나타낸다. 즉, 이는 스팸 검출 시스템의 검출 능력을 나타낸다.

[0092] 도 12b는 본 발명의 일 실시예에 따른 팩스 스팸 차단 방법의 세 가지 분류 방식의 Pre_spam 결과를 나타낸 표이다.

[0093] 도 12b에 도시된 바와 같이, RB 분류 방법의 Pre_spam은 RB에 사용된 특징들의 수에 따라 증가한다. 반면, SVM 및 NB의 Pre_spam 결과는 특징들의 모든 수에서 100%를 나타낸다.

[0094] 다시 도 11로 돌아가서, Rec_spam은 시스템이 할 수 있는 한 최대한 많은 스팸 문서들을 검출하는지를 나타낸다. 즉, 이는 전체 스팸 문서 중에서 얼마나 많은 스팸 팩스 문서를 검출할 수 있는지에 대한 능력을 나타낸다.

[0095] 도 12c는 본 발명의 일 실시예에 따른 팩스 스팸 차단 방법의 세 가지 분류 방식의 Rec_spam 결과를 나타낸 표이다.

[0096] 도 12c에 도시된 바와 같이, RB 분류 방법, SVM 분류 방법 및 NB 분류 방법의 Rec_spam은 거의 동일하다. 즉, RB의 ACC 및 Pre_spam이 다른 것들보다 낮았음에도 불구하고, RB의 Rec_spam은 다른 분류 방법보다 더 높았다 이는 RB가 좋지 않은 성능을 가졌음을 나타낸다.

[0097] 다시 도 11로 돌아가서, Rec_norm은 거짓 양성(false positive) 확률을 나타낸다. 즉 Rec_norm이 높을수록, 낮은 거짓 양성 확률을 나타낼 수 있다.

[0098] 도 12d는 본 발명의 일 실시예에 따른 팩스 스팸 차단 방법의 세 가지 분류 방식의 Rec_norm 결과를 나타낸 표이다.

[0099] 도 12d에 도시된 바와 같이, NB는 단지10 특징들이 사용되었을 때, 100% 결과를 달성했고, RB는 28.99%, SVM은

78.77%의 결과를 달성했다.

[0100] 위의 결과들을 토대로, 정밀도와 리콜의 조합값을 나타내는 F-measure를 계산할 수 있다.

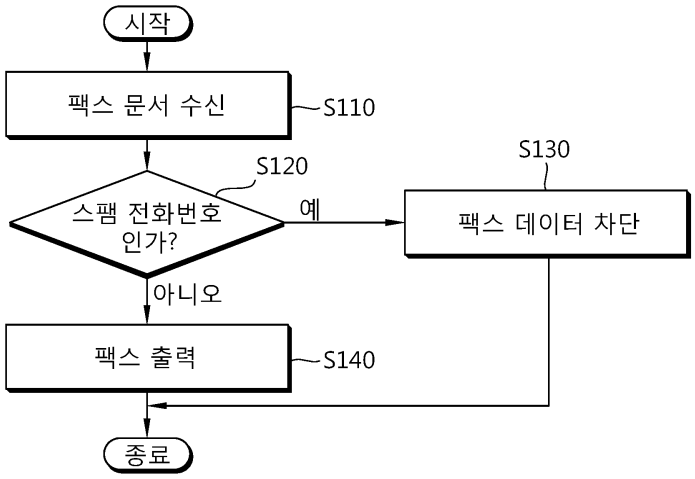
[0101] 도 13은 고급 스팸 공격에서의 본 발명의 일 실시예에 따른 팩스 스팸 차단 방법의 세 가지 분류 방식의 F-measure를 비교한 그래프이다.

[0102] 도 13에 도시된 바와 같이, RB 및 SVM의 F-measure는 특징들의 변화에 영향을 많이 받는 특징이 있다. 반면, NB의 F-measure는 전체 x축(특징들의 수)에서 안정적인 결과를 나타낸다. 따라서, 팩스 스팸 검출에 NB를 사용하는 것을 추천할 수 있다.

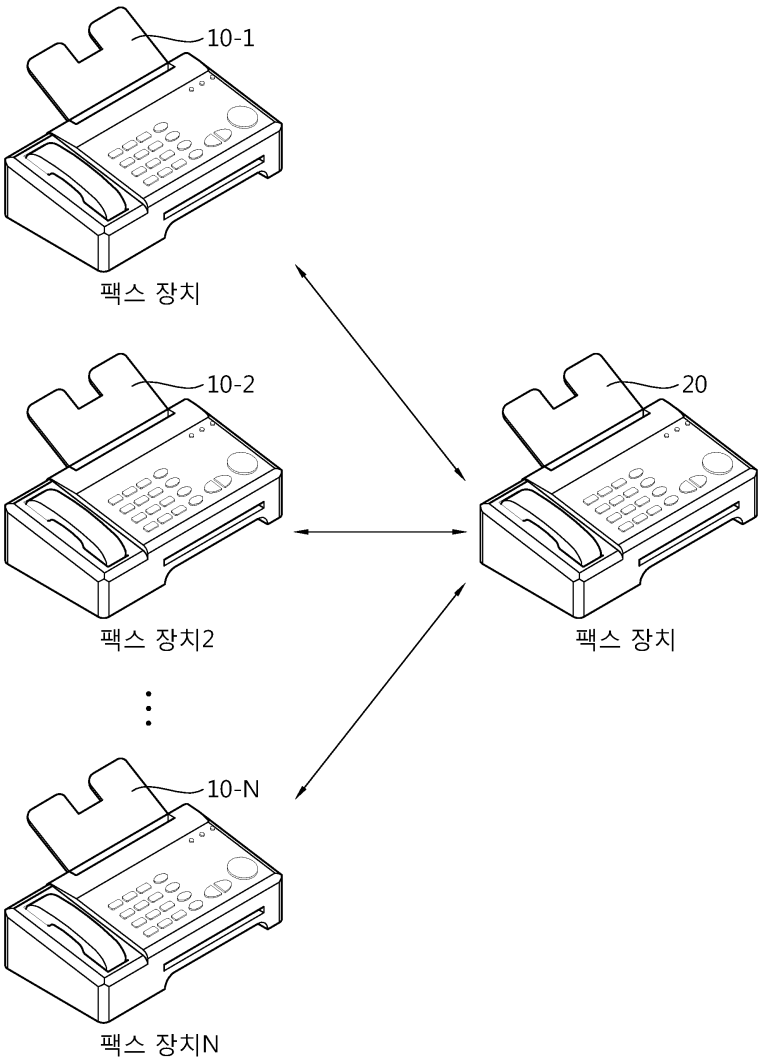
[0103] 이상 도면 및 실시예를 참조하여 설명하였지만, 본 발명의 보호범위가 상기 도면 또는 실시예에 의해 한정되는 것을 의미하지는 않으며 해당 기술 분야의 숙련된 당업자는 하기의 특허 청구의 범위에 기재된 본 발명의 사상 및 영역으로부터 벗어나지 않는 범위 내에서 본 발명을 다양하게 수정 및 변경시킬 수 있음을 이해할 수 있을 것이다.

도면

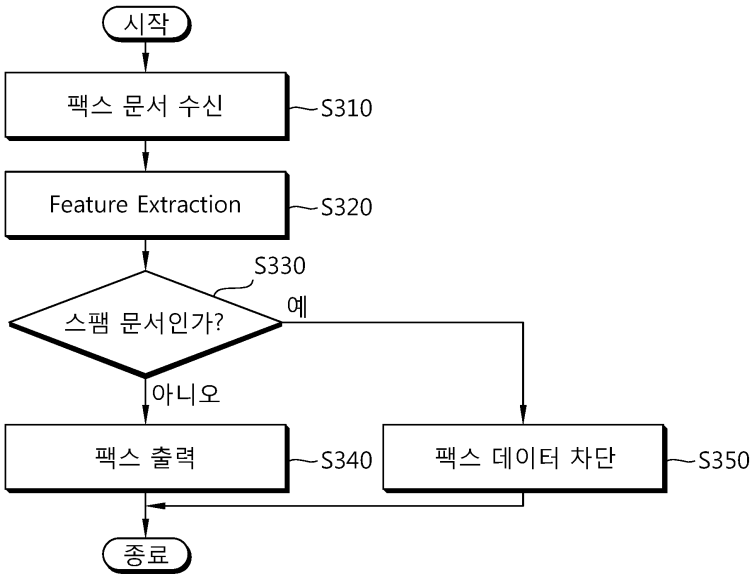
도면1



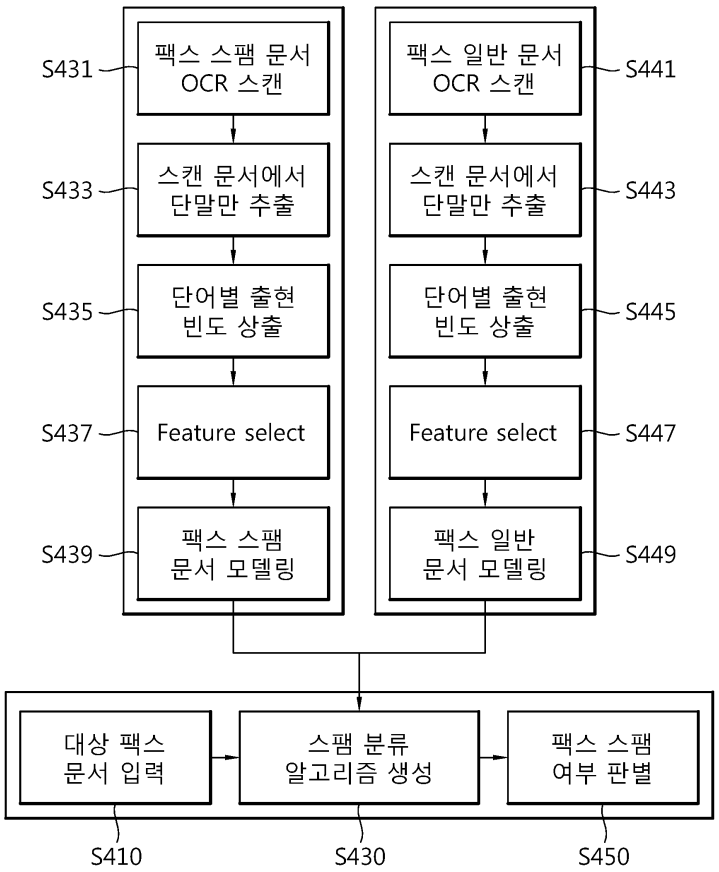
도면2



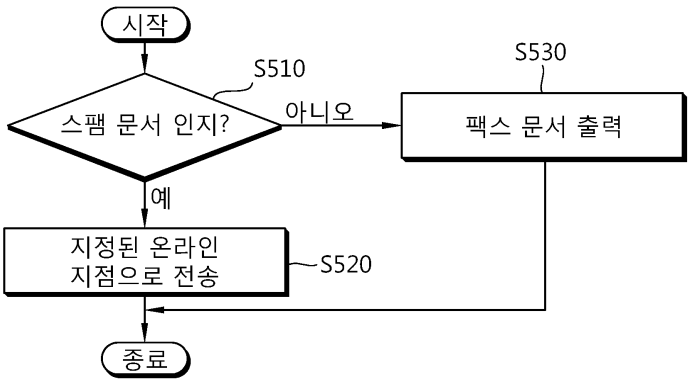
도면3


시작
팩스 문서 수신
S310
Feature Extraction
S320
S330
스팸 문서인가?
예
아니오
팩스 출력
S340
팩스 데이터 차단
S350
종료

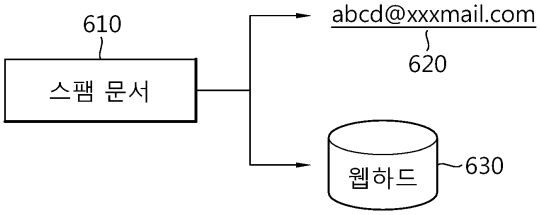
도면4


S431
팩스 스팸 문서 OCR 스캔
S433
스캔 문서에서 단말만 추출
S435
단어별 출현 빈도 상출
S437
Feature select
S439
팩스 스팸 문서 모델링
S441
팩스 일반 문서 OCR 스캔
S443
스캔 문서에서 단말만 추출
S445
단어별 출현 빈도 상출
S447
Feature select
S449
팩스 일반 문서 모델링
대상 팩스 문서 입력
스팸 분류 알고리즘 생성
팩스 스팸 여부 판별
S410
S430
S450

도면5

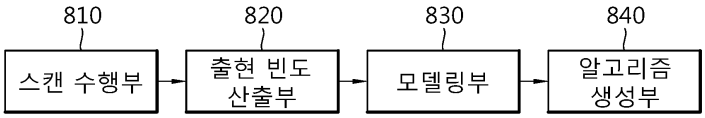


도면6

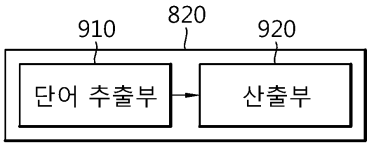


도면7

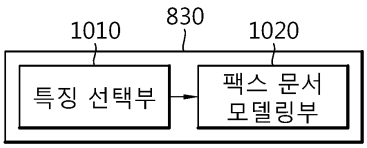
도면8



도면9



도면10



도면11

	Spam	Normal
Is Spam	A	B
Is Normal	C	D

도면12a

# of features	10	20	30	40	50	60	70	80	90	100
RB	55.35	66.79	70.11	72.32	72.69	74.91	75.65	77.86	78.23	80.07
SVM	91.14	90.41	90.77	90.41	90.77	90.70	90.77	90.77	90.77	90.77
NB	91.79	91.06	91.43	91.03	91.72	91.42	91.45	91.33	91.69	91.49

도면12b

# of features	10	20	30	40	50	60	70	80	90	100
RB	52.88	62.01	65.29	67.68	68.10	70.70	71.61	74.50	74.67	77.24
SVM	100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00
NB	100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00

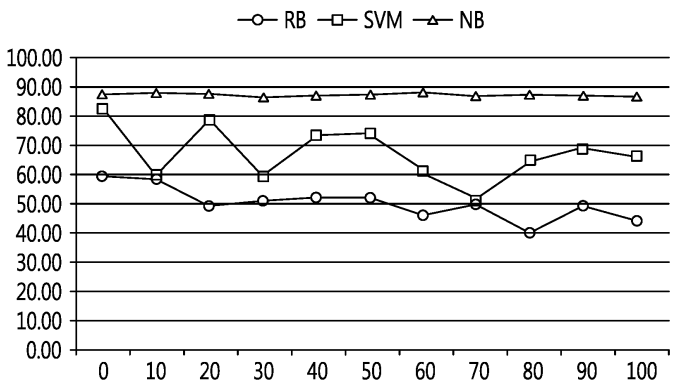
도면12c

# of features	10	20	30	40	50	60	70	80	90	100
RB	82.71	83.46	83.46	83.46	83.46	83.46	83.46	83.46	84.21	84.21
SVM	81.95	80.45	81.20	80.45	81.20	81.20	81.20	81.20	81.20	81.20
NB	83.21	82.45	82.26	81.91	82.99	82.39	82.30	82.59	82.83	82.84

도면12d

# of features	10	20	30	40	50	60	70	80	90	100
RB	28.99	50.72	57.25	61.59	62.32	66.67	68.12	72.46	72.46	76.09
SVM	78.77	76.58	77.69	76.58	77.69	77.69	77.69	77.69	77.69	77.69
NB	100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00	100.00

도면13


RB
SVM
NB
100.00
90.00
80.00
70.00
60.00
50.00
40.00
30.00
20.00
10.00
0.00
0
10
20
30
40
50
60
70
80
90
100