(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2016-0000574
(43) 공개일자 2016년01월05일

(51) 국제특허분류(Int. Cl.)
G06F 21/00 (2006.01) *G06T 1/00* (2006.01)
H04W 4/12 (2009.01)
(21) 출원번호 10-2014-0077664
(22) 출원일자 2014년06월24일
심사청구일자 2014년06월24일

(71) 출원인
경희대학교 산학협력단
경기도 용인시 기흥구 덕영대로 1732 (서천동, 경희대학교 국제캠퍼스내)
(72) 발명자
홍충선
경기도 용인시 수지구 상현로 30-10 상현마을 성원상떼빌 233-101 (상현동, 상현마을성원상떼빌아파트)
강효성
경북 경주시 광중길 73-16, 110동 203호 (황성동, 현진에버빌)
(74) 대리인
김연권

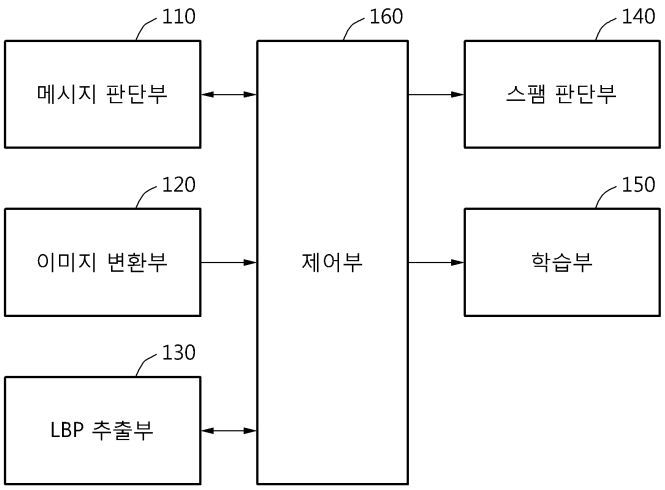
전체 청구항 수 : 총 10 항

(54) 발명의 명칭 **이미지 스팸 필터링 장치 및 방법**

(57) 요 약

수신된 메시지가 이미지 메시지인지 여부를 판단하고, 상기 메시지가 이미지 메시지인 경우, 상기 메시지에 포함된 이미지를 이진화 하여 그레이 스케일로 변환하고, 상기 그레이 스케일로 변환된 이미지로 LBP(Local Binary Pattern) 정보를 추출하고, SVM(Support Vector Machine) 분류 알고리즘을 이용하여 상기 추출된 LBP 정보를 분류하고, 상기 분류된 결과를 기반으로 상기 메시지가 이미지 스팸인지 여부를 판단하는 이미지 스팸 필터링 장치 및 방법을 제공한다.

대 표 도 - 도1



이 발명을 지원한 국가연구개발사업
과제고유번호 20131558
부처명 미래창조과학부
연구관리전문기관 한국연구재단
연구사업명 차세대정보/컴퓨팅기술개발사업
연구과제명 실시간 M2M 네트워크 관리기술
기 여 율 1/1
주관기관 경희대학교 산학협력단
연구기간 2013.07.01 ~ 2014.06.30

명 세 서

청구범위

청구항 1

수신된 메시지가 이미지 메시지인지 여부를 판단하는 메시지 판단부;

상기 메시지가 이미지 메시지인 경우, 상기 메시지에 포함된 이미지를 이진화 하여 그레이 스케일로 변환하는 이미지 변환부;

상기 그레이 스케일로 변환된 이미지로 LBP(Local Binary Pattern) 정보를 추출하는 LBP 추출부; 및

SVM(Support Vector Machine) 분류 알고리즘을 이용하여 상기 추출된 LBP 정보를 분류하고, 상기 분류된 결과를 기반으로 상기 메시지가 이미지 스팸인지 여부를 판단하는 스팸 판단부

를 포함하는 이미지 스팸 필터링 장치.

청구항 2

제1항에 있어서,

상기 스팸 판단부는,

상기 변환된 이미지의 그레이 레벨을 분석하여 미리 설정된 레벨 사이에서 미리 설정된 빈도 수를 가지는 경우, 상기 메시지를 이미지 스팸으로 결정하는

이미지 스팸 필터링 장치.

청구항 3

제1항에 있어서,

상기 추출된 LBP 정보로부터 추출된 패턴 중 일부 패턴을 학습 데이터로 선정하고, 상기 선정된 학습 데이터를 SVM(Support Vector Machine)을 통하여 학습하는 학습부

를 더 포함하는 이미지 스팸 필터링 장치.

청구항 4

제3항에 있어서,

상기 스팸 판단부는,

미리 학습된 전체 이미지 스팸의 패턴을 기반으로 상기 학습된 학습 데이터의 경계(Hyperplane)를 기준으로 하여, 상기 메시지가 이미지 스팸인지 여부를 판단하는

이미지 스팸 필터링 장치.

청구항 5

제1항에 있어서,

상기 LBP 추출부는 상기 변환된 이미지의 픽셀 단위 별로 상기 LBP 정보에 가중치를 적용하여 eLBP(edge-LBP) 정보를 연산하고,

상기 스팸 판단부는 SVM(Support Vector Machine) 분류 알고리즘을 이용하여 상기 추출된 eLBP 정보를 분류하고, 상기 분류된 결과를 기반으로 상기 메시지가 이미지 스팸인지 여부를 판단하는

이미지 스팸 필터링 장치.

청구항 6

수신된 메시지가 이미지 메시지인지 여부를 판단하는 단계;

상기 메시지가 이미지 메시지인 경우, 상기 메시지에 포함된 이미지를 이진화 하여 그레이 스케일로 변환하는 단계;

상기 그레이 스케일로 변환된 이미지로 LBP(Local Binary Pattern) 정보를 추출하는 단계; 및

SVM(Support Vector Machine) 분류 알고리즘을 이용하여 상기 추출된 LBP 정보를 분류하고, 상기 분류된 결과를 기반으로 상기 메시지가 이미지 스팸인지 여부를 판단하는 단계

를 포함하는 이미지 스팸 필터링 방법.

청구항 7

제6항에 있어서,

상기 변환된 이미지의 그레이 레벨을 분석하여 미리 설정된 레벨 사이에서 미리 설정된 빈도 수를 가지는 경우, 상기 메시지를 이미지 스팸으로 결정하는 단계

를 더 포함하는 이미지 스팸 필터링 방법.

청구항 8

제6항에 있어서,

상기 추출된 LBP 정보로부터 추출된 패턴 중 일부 패턴을 학습 데이터로 선정하는 단계; 및

상기 선정된 학습 데이터를 SVM(Support Vector Machine)을 통하여 학습하는 단계

를 더 포함하는 이미지 스팸 필터링 방법.

청구항 9

제8항에 있어서,

미리 학습된 전체 이미지 스팸의 패턴을 기반으로 상기 학습된 학습 데이터의 경계(Hyperplane)를 기준으로 하여, 상기 메시지가 이미지 스팸인지 여부를 판단하는 단계

를 더 포함하는 이미지 스팸 필터링 방법.

청구항 10

제6항에 있어서,

상기 변환된 이미지의 픽셀 단위 별로 상기 LBP 정보에 가중치를 적용하여 eLBP(edge-LBP) 정보를 연산하는 단계; 및

SVM(Support Vector Machine) 분류 알고리즘을 이용하여 상기 추출된 eLBP 정보를 분류하고, 상기 분류된 결과를 기반으로 상기 메시지가 이미지 스팸인지 여부를 판단하는 단계

를 더 포함하는 이미지 스팸 필터링 방법.

발명의 설명

기 술 분 야

[0001] 본 발명의 실시예들은 이미지 이진화를 이용한 이미지 스팸 필터링 장치 및 방법에 관한 것이다.

배 경 기 술

[0002] 인터넷의 급속한 성장과 더불어 전자 메일 사용자의 수가 증가하면서 인터넷 상에 개인 전자 메일 주소의 노출로 인한 스팸 메시지의 양도 덩달아 증가하게 되었다. 이러한 현상은 메일 사용자에게 악용되어 바이러스 전파 및 개인정보 노출의 원인이 되고 있다.

[0003] 따라서, 스팸 메시지를 차단하는 다양한 방법들이 제시되고 있는 실정이다.

[0004] 그 대표적인 방법 중 하나가 텍스트 기반 스팸 필터링 방법이다. 텍스트 기반 스팸 필터링은 수신된 메시지의 텍스트 내용을 추출하여 해당 텍스트 내용과 스팸으로 분류한 텍스트의 내용을 서로 비교하여 수신된 메시지의 스팸 여부를 판단하는 방식이다.

[0005] 현재 모바일 문자 메시지와 웹 상의 전자 메일에 탑재된 스팸 메시지 필터링 알고리즘은 대부분 텍스트 기반이다.

[0006] 텍스트 기반 스팸 필터링 기법은 메시지가 수신되면 해당 메시지의 내용에서 텍스트를 추출하고, 스팸 텍스트로 판단되어 분류된 데이터 베이스에서 스팸 텍스트 데이터를 가져와 수신된 메시지의 텍스트 내용과 비교한다.

[0007] 그리고, 비교한 결과에서 최종적으로 일치하는 정보가 있는 경우 해당 메시지를 스팸으로 판단할 수 있다.

[0008] 이때, 텍스트 기반의 스팸 필터링 기법은 전 처리기 단계를 거칠 수 있으며, 텍스트에서 스팸으로 등록된 단어들과 비교하여 필터링하기 위해 전처리 단계에서 텍스트 메시지의 특수 문자를 제거, 문장 사이 자동 띄어쓰기 추가, 수사어절 표준화, 실제 사전에 없는 은어와 같은 불용어 제거 단계를 우선적으로 거칠 수 있다. 텍스트 기반의 스팸 필터링 기법은 이러한 전처리 단계를 거친 후 필터링 단어의 패턴으로 학습된 SVM(Support Vector Machine)을 통해 상기 텍스트 메시지의 스팸 여부를 판단할 수 있다.

[0009] 기존의 텍스트 기반 스팸 필터링 기법은 수신된 메시지에서 텍스트 추출이 가능하다는 전제하에 동작하는 알고리즘이다. 하지만, 텍스트가 거의 포함되어 있지 않거나, 이미지 또는 HTML 만을 포함하는 이미지 스팸(Image Spam)의 경우, 비교 판단할 수 있는 텍스트가 거의 없기 때문에 기존 텍스트 기반 스팸 필터링 기법으로 차단할 수 없는 어려움이 있다.

발명의 내용

해결하려는 과제

[0010] 본 발명의 일실시예는 메시지 내용이 텍스트가 아닌 이미지 형태로 되어 있어 스팸 필터링으로 차단하기 어려웠던 이미지 스팸 메시지를 필터링 하는 장치 및 방법을 제공한다.

[0011] 본 발명의 일실시예는 모바일 기기를 통한 문자 메시지, 인터넷 상의 웹 계정을 통한 전자 메일 등에 포함된 이미지 스팸을 차단하는 방법을 제공한다.

[0012] 본 발명의 일실시예는 이미지 스팸으로 유포되는 바이러스 및 악성 프로그램에 대한 예방이 가능하다.

과제의 해결 수단

[0013] 본 발명의 일실시예에 따른 이미지 스팸 필터링 장치는 수신된 메시지가 이미지 메시지인지 여부를 판단하는 메시지 판단부, 상기 메시지가 이미지 메시지인 경우, 상기 메시지에 포함된 이미지를 이진화 하여 그레이 스케일

로 변환하는 이미지 변환부, 상기 그레이 스케일로 변환된 이미지로 LBP(Local Binary Pattern) 정보를 추출하는 LBP 추출부, 및 SVM(Support Vector Machine) 분류 알고리즘을 이용하여 상기 추출된 LBP 정보를 분류하고, 상기 분류된 결과를 기반으로 상기 메시지가 이미지 스팸인지 여부를 판단하는 스팸 판단부를 포함한다.

[0014] 본 발명의 일측에 따르면, 상기 스팸 판단부는 상기 변환된 이미지의 그레이 레벨을 분석하여 미리 설정된 레벨 사이에서 미리 설정된 빈도 수를 가지는 경우, 상기 메시지를 이미지 스팸으로 결정할 수 있다.

[0015] 본 발명의 일측에 따른 이미지 스팸 필터링 장치는 상기 추출된 LBP 정보로부터 추출된 패턴 중 일부 패턴을 학습 데이터로 선정하고, 상기 선정된 학습 데이터를 SVM(Support Vector Machine)을 통하여 학습하는 학습부를 더 포함할 수 있다.

[0016] 본 발명의 일측에 따르면, 상기 스팸 판단부는 미리 학습된 전체 이미지 스팸의 패턴을 기반으로 상기 학습된 학습 데이터의 경계(Hyperplane)를 기준으로 하여, 상기 메시지가 이미지 스팸인지 여부를 판단할 수 있다.

[0017] 본 발명의 일측에 따르면, 상기 LBP 추출부는 상기 변환된 이미지의 픽셀 단위 별로 상기 LBP 정보에 가중치를 적용하여 eLBP(edge-LBP) 정보를 연산하고, 상기 스팸 판단부는 SVM(Support Vector Machine) 분류 알고리즘을 이용하여 상기 추출된 eLBP 정보를 분류하고, 상기 분류된 결과를 기반으로 상기 메시지가 이미지 스팸인지 여부를 판단할 수 있다.

[0018] 본 발명의 일실시예에 따른 이미지 스팸 필터링 방법은 수신된 메시지가 이미지 메시지인지 여부를 판단하는 단계, 상기 메시지가 이미지 메시지인 경우, 상기 메시지에 포함된 이미지를 이진화 하여 그레이 스케일로 변환하는 단계, 상기 그레이 스케일로 변환된 이미지로 LBP(Local Binary Pattern) 정보를 추출하는 단계, 및 SVM(Support Vector Machine) 분류 알고리즘을 이용하여 상기 추출된 LBP 정보를 분류하고, 상기 분류된 결과를 기반으로 상기 메시지가 이미지 스팸인지 여부를 판단하는 단계를 포함한다.

[0019] 본 발명의 일측에 따른 이미지 스팸 필터링 방법은 상기 변환된 이미지의 그레이 레벨을 분석하여 미리 설정된 레벨 사이에서 미리 설정된 빈도 수를 가지는 경우, 상기 메시지를 이미지 스팸으로 결정하는 단계를 더 포함할 수 있다.

[0020] 본 발명의 일측에 따른 이미지 스팸 필터링 방법은 상기 추출된 LBP 정보로부터 추출된 패턴 중 일부 패턴을 학습 데이터로 선정하는 단계, 및 상기 선정된 학습 데이터를 SVM(Support Vector Machine)을 통하여 학습하는 단계를 더 포함할 수 있다.

[0021] 본 발명의 일측에 따른 이미지 스팸 필터링 방법은 미리 학습된 전체 이미지 스팸의 패턴을 기반으로 상기 학습된 학습 데이터의 경계(Hyperplane)를 기준으로 하여, 상기 메시지가 이미지 스팸인지 여부를 판단하는 단계를 더 포함할 수 있다.

[0022] 본 발명의 일측에 따른 이미지 스팸 필터링 방법은 상기 변환된 이미지의 픽셀 단위 별로 상기 LBP 정보에 가중치를 적용하여 eLBP(edge-LBP) 정보를 연산하는 단계, 및 SVM(Support Vector Machine) 분류 알고리즘을 이용하여 상기 추출된 eLBP 정보를 분류하고, 상기 분류된 결과를 기반으로 상기 메시지가 이미지 스팸인지 여부를 판단하는 단계를 더 포함할 수 있다.

발명의 효과

[0023] 본 발명의 일실시예에 따르면 메시지 내용이 텍스트가 아닌 이미지 형태로 되어 있어 스팸 필터링으로 차단하기 어려웠던 이미지 스팸 메시지를 필터링 할 수 있다.

[0024] 본 발명의 일실시예에 따르면 모바일 기기를 통한 문자 메시지, 인터넷 상의 웹 계정을 통한 전자 메일 등에 포함된 이미지 스팸을 차단할 수 있다.

[0025] 본 발명의 일실시예에 따르면 이미지 스팸으로 유포되는 바이러스 및 악성 프로그램에 대한 예방이 가능하다.

도면의 간단한 설명

[0026] 도 1은 본 발명의 일실시예에 따른 이미지 스팸 필터링 장치의 구성을 도시한 블록도이다.

도 2는 본 발명의 일측에 따른 이미지 변환의 예를 도시한 도면이다.

도 3은 본 발명의 일측에 따른 LBP 정보를 추출하는 예를 도시한 도면이다.

도 4는 본 발명의 일측에 따른 eLBP(edge-LBP) 특징 추출 과정을 도시한 도면이다.

도 5는 SVM의 범주를 분류한 예를 도시한 도면이다.

도 6은 SVM 분류 알고리즘에서 초평면(Hyperplane)을 선택하는 예를 도시한 도면이다.

도 7은 본 발명의 일측에 따른 이미지 스팸 필터링 방법을 도시한 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0027] 이하 첨부 도면들 및 첨부 도면들에 기재된 내용들을 참조하여 본 발명의 실시예를 상세하게 설명하지만, 본 발명이 실시예에 의해 제한되거나 한정되는 것은 아니다.

[0028] 한편, 본 발명을 설명함에 있어서, 관련된 공지 기능 또는 구성에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는, 그 상세한 설명을 생략할 것이다. 그리고, 본 명세서에서 사용되는 용어(terminology)들은 본 발명의 실시예를 적절히 표현하기 위해 사용된 용어들로서, 이는 사용자, 운용자의 의도 또는 본 발명이 속하는 분야의 관례 등에 따라 달라질 수 있다. 따라서, 본 용어들에 대한 정의는 본 명세서 전반에 걸친 내용을 토대로 내려져야 할 것이다.

[0029] 본 발명의 일실시예는 메시지 내용이 텍스트가 아닌 이미지 형태로 되어 있어 스팸 필터링으로 차단하기 어려웠던 이미지 스팸 메시지를 필터링 하는 장치 및 방법을 제공한다.

[0030] 도 1은 본 발명의 일실시예에 따른 이미지 스팸 필터링 장치의 구성을 도시한 블록도이다.

[0031] 도 1을 참조하면, 본 발명에 따른 일실시예 따른 이미지 스팸 필터링 장치는 메시지 판단부(110), 이미지 변환부(120), LBP 추출부(130), 스팸 판단부(140), 및 학습부(150)을 포함한다.

[0032] 본 발명의 일측에 따르면, 이미지 스팸 필터링 장치는 제어부(160)를 포함할 수 있으며, 제어부(160)는 이미지 스팸 필터링 장치의 전반적인 동작을 제어할 수 있다. 예를 들어, 제어부(160)는 연결된 모듈 간의 데이터를 송수신하여 다른 모듈로 전달하거나, 제어 데이터를 생성하여 각각의 모듈을 제어하는 역할을 담당할 수 있다. 또한, 각각의 모듈은 제어부(160)의 제어에 의하여 구동 될 수도 있고, 제어부(160)와 별도로 독립적으로 구현될 수도 있다.

[0033] 판단부(110)는 수신된 메시지가 이미지 메시지인지 여부를 판단한다.

[0034] 예를 들어, 판단부(110)는 수신된 메시지에 이미지 파일이 포함되었거나, 텍스트 파일이 포함되었더라도 이미지 파일의 비율이 높은 경우에 상기 메시지를 이미지 메시지로 판단할 수도 있다.

[0035] 이미지 변환부(120)는 상기 메시지가 이미지 메시지인 경우, 상기 메시지에 포함된 이미지를 이진화 하여 그레이 스케일로 변환한다.

[0036] 예를 들어, 이미지 변환부(120)는 상기 메시지가 이미지 메시지로 판단 되면 상기 이미지 메시지에 포함된 이미지 파일을 이진화하여 그레이 스케일(예를 들어, 이미지를 이진화 하는 방식)로 변환할 수 있다.

[0037] 도 2는 본 발명의 일측에 따른 이미지 변환의 예를 도시한 도면이다.

[0038] 도 2를 참조하면, 수신된 메시지에 포함된 이미지가 컬러 이미지(211, 212)인 경우, 이미지 변환부(120)는 상기 컬러 이미지(211, 212)를 이진화 하여 그레이 스케일의 이미지(221, 222)로 변환할 수 있다.

[0039] LBP 추출부(130)는 상기 그레이 스케일로 변환된 이미지로 LBP(Local Binary Pattern) 정보를 추출한다.

[0040] 도 3은 본 발명의 일측에 따른 LBP 정보를 추출하는 예를 도시한 도면이다.

[0041] 도 2 및 도 3을 참조하면, LBP 추출부(130)는 도 2의 그레이 스케일의 이미지(221, 222)로부터 이미지의 질감 정보를 이진화 데이터로 표현하는 LBP 정보를 추출하여 히스토그램화(311, 312) 할 수 있다. LBP는 이미지 정보를 2진화 패턴으로 추출하는 방법으로 이미지 질감에 대한 특징 표현을 할 수 있다.

[0042] 본 발명의 일측에 따르면, LBP 추출부(130)는 이미지 내에서 적은 차원을 가지면서 많은 질감 정보를 표현하는 eLBP(edge-LBP)를 적용할 수도 있다.

[0043] 본 발명의 이해를 돕고자 eLBP(edge-LBP) 특징 추출 기법을 아래와 같이 설명하도록 한다. eLBP 특징 추출 기법은 질감의 경계 정보를 표현하기 위해 고안된 방식이다.

[0044] 도 4는 본 발명의 일측에 따른 eLBP(edge-LBP) 특징 추출 과정을 도시한 도면이다.

[0045] 도 4를 참조하면, eLBP(edge-LBP) 특징 추출 기법은 3ㅅ3 픽셀 블록 단위(410)로 중심 화소의 화소 값이 중심 화소 및 이웃 화소의 화소 값의 차보다 크면 1 작으면 0의 값으로 표현할 수 있다(420).

[0046] 상기 표현된 픽셀 블록 단위(420)의 값에 가중치를 각각 곱하여 수직, 수평 성분 별로 따로 더할 수 있다. 예를 들어, 상기 표현된 픽셀 블록 단위(420)의 값에 1, 1, 2, 2, 4, 4, 8, 8의 가중치를 각각 곱하여 수직, 수평 성분 별로 더할 수 있다(430, 440).

[0047] [수학식 1]

[0048] $eLBP_{V-h} = 2$

[0049] $eLBP_{diag} = 2 + 4 = 6$

[0050] [수학식 2]

[0051] $\therefore eLBP_{total} = eLBP_{V-h} + eLBP_{diag} = 2 + 6 = 8$

[0052] 이때, 상기 $eLBP_{V-h}$는 화소의 수직, 수평 정보를 표현한 값이고, $eLBP_{diag}$는 화소의 대각선 정보를 표현한 값이다.

[0053] 최종적으로 이미지의 $eLBP_{total}$ 값은 $eLBP_{V-h}$와 $eLBP_{diag}$를 더하여 표현할 수 있다.

[0054] 스팸 판단부(140)는 SVM(Support Vector Machine) 분류 알고리즘을 이용하여 상기 추출된 LBP 정보를 분류하고, 상기 분류된 결과를 기반으로 상기 메시지가 이미지 스팸인지 여부를 판단한다.

[0055] 예를 들어, 스팸 판단부(140)는 상기 변환된 이미지의 그레이 레벨을 분석하여 미리 설정된 레벨 사이에서 미리 설정된 빈도 수를 가지는 경우, 상기 메시지를 이미지 스팸으로 결정할 수 있다.

[0056] 구체적으로, 이미지 스팸은 도 3에 도시된 바와 같이 평균적으로 그레이 레벨이 155~170, 220~230 사이에서 높은 해당 그레이 레벨의 빈도 수를 가질 수 있다. 이런 특징들은 SVM의 학습에서 정확한 분류 임계 값을 정하는 기준이 될 수 있으며, 이미지의 스팸 여부를 결정짓는 중요한 기준이 될 수 있다.

[0057] 또한, LBP 추출부(130)는 상기 변환된 이미지의 픽셀 단위 별로 상기 LBP 정보에 가중치를 적용하여 eLBP(edge-LBP) 정보를 연산하고, 스팸 판단부(140)는 SVM(Support Vector Machine) 분류 알고리즘을 이용하여 상기 추출된 eLBP 정보를 분류하고, 상기 분류된 결과를 기반으로 상기 메시지가 이미지 스팸인지 여부를 판단할 수 있다.

[0058] 다시 도 1을 참조하면, 학습부(150)는 상기 추출된 LBP 정보로부터 추출된 패턴 중 일부 패턴을 학습 데이터로 선정하고, 상기 선정된 학습 데이터를 SVM(Support Vector Machine)을 통하여 학습할 수 있다.

[0059] 스팸 판단부(140)는 미리 학습된 전체 이미지 스팸의 패턴을 기반으로 상기 학습된 학습 데이터의 경계(Hyperplane)를 기준으로 하여, 상기 메시지가 이미지 스팸인지 여부를 판단할 수 있다.

[0060] 본 발명의 전반에 걸쳐 언급되는 SVM(Support Vector Machine) 이라 함은 머신 러닝(Machine Learning) 기법 중 하나로, SVM(Support Vector Machine) 분류 알고리즘은 주어진 자료에 대해서 그 자료들을 분리하는 지점을 찾는 것을 목적으로 하는 알고리즘 방법이다.

[0061] 도 5는 SVM의 범주를 분류한 예를 도시한 도면이고, 도 6은 SVM 분류 알고리즘에서 초평면(Hyperplane)을 선택하는 예를 도시한 도면이다.

[0062] 도 5 및 6을 참조하면, SVM 분류 알고리즘은 벡터 공간에 표시될 수 있으며 선형이든 비선형이든 분류 할 수 있는 방법이다. 도 5 및 도 6과 같은 벡터들 중 같은 범주를 기준으로 바깥으로 위치한 벡터들의 연결선으로 이루어진 다각형을 볼록 껍질(convex hull)이라 하며, 상기 convex hull 안에 다른 벡터들은 그룹을 분류하는데 영향을 미치지 않지만 가장 바깥에 있는 위치한 벡터들이 큰 영향을 미칠 수 있다.

[0063] 도 5에 도시된 바와 같이, 가장 바깥에 위치한 벡터들을 서포트 벡터(Support Vector)라 하며, 서포트 벡터들을

가르는 선 및 면을 초평면(hyperplane)이라고 한다.

[0064] 도 6에 도시된 바와 같이, 초평면(H1, H2, H3)은 복수개가 생길 수 있으나, 그 중에서 서포트 벡터와 가장 먼 거리를 가진 초평면인 H2가 두 그룹을 효과적으로 분류할 수 있다.

[0065] 학습부(150)는 eLBP 특징 추출 기법을 통해 추출된 스팸 패턴, 비스팸 패턴에서 무작위로 일부 패턴만을 추출하여 학습 데이터로 선정할 수도 있다. 예를 들어, 학습부(150)는 스팸 패턴, 비스팸 패턴에서 무작위로 약 20%만을 추출하여 학습 데이터로 선정할 수도 있다.

[0066] 본 발명의 일측에 따르면, 선정된 학습 데이터는 SVM(Support Vector Machine) 학습에 활용될 수 있으며, 스팸 판단부(140)는 전체 이미지 스팸의 패턴을 입력 받아 학습된 데이터로부터 선별된 초평면을 기준으로 수신된 메시지가 이미지 스팸인지 여부를 결정할 수 있다.

[0067] 아래에서는 본 발명의 일실시예에 따른 이미지 스팸 필터링 방법을 설명하도록 한다.

[0068] 본 발명의 일측에 따른 이미지 스팸 필터링 방법은 전술한 이미지 스팸 필터링 장치를 이용하여 수행될 수 있는 바, 이미지 스팸 필터링 장치의 관점에서 설명하도록 한다.

[0069] 도 7은 본 발명의 일측에 따른 이미지 스팸 필터링 방법을 도시한 흐름도이다.

[0070] 도 7을 참조하면, 이미지 스팸 필터링 장치는 메시지를 수신하고(710), 수신된 메시지가 이미지 메시지인지 여부를 판단한다(720).

[0071] 이미지 스팸 필터링 장치는 상기 메시지가 이미지 메시지인 경우, 상기 메시지에 포함된 이미지를 이진화 하여 그레이 스케일로 변환한다(730).

[0072] 이미지 스팸 필터링 장치는 상기 그레이 스케일로 변환된 이미지로 LBP(Local Binary Pattern) 정보를 추출한다(740).

[0073] 이미지 스팸 필터링 장치는 SVM(Support Vector Machine) 분류 알고리즘을 이용하여 상기 추출된 LBP 정보를 분류한다(750).

[0074] 이미지 스팸 필터링 장치는 상기 분류된 결과를 기반으로 상기 메시지가 이미지 스팸인지 여부를 판단한다(760).

[0075] 이미지 스팸 필터링 장치는 상기 변환된 이미지의 그레이 레벨을 분석하여 미리 설정된 레벨 사이에서 미리 설정된 빈도 수를 가지는 경우, 상기 메시지를 이미지 스팸으로 결정할 수 있다.

[0076] 또한, 이미지 스팸 필터링 장치는 상기 추출된 LBP 정보로부터 추출된 패턴 중 일부 패턴을 학습 데이터로 선정하고, 상기 선정된 학습 데이터를 SVM(Support Vector Machine)을 통하여 학습할 수 있다(770).

[0077] 이미지 스팸 필터링 장치는 미리 학습된 전체 이미지 스팸의 패턴을 기반으로 상기 학습된 학습 데이터의 경계(Hyperplane)를 기준으로 하여, 상기 메시지가 이미지 스팸인지 여부를 판단할 수도 있다.

[0078] 이미지 스팸 필터링 장치는 상기 변환된 이미지의 픽셀 단위 별로 상기 LBP 정보에 가중치를 적용하여 eLBP(edge-LBP) 정보를 연산하고, SVM(Support Vector Machine) 분류 알고리즘을 이용하여 상기 추출된 eLBP 정보를 분류하고, 상기 분류된 결과를 기반으로 상기 메시지가 이미지 스팸인지 여부를 판단할 수 있다.

[0079] 본 발명의 일측에 따른 이미지 스팸 필터링 방법은 모바일 기기를 통한 문자 메시지, 인터넷 상의 웹 계정을 통한 전자 메일의 이미지 스팸을 차단시킬 수 있다.

[0080] 본 발명의 일측에 따른 이미지 스팸 필터링 방법은 이미지 스팸으로 유포되는 바이러스, 악성 프로그램에 대한 배포를 예방할 수 있다.

[0081] 본 발명의 일측에 따른 이미지 스팸 필터링 방법은 이미지 스팸의 차단율을 높이고, 텍스트 기반 스팸 필터링 시스템을 우회하여 배포되는 악성 프로그램과 바이러스의 배포 차단율을 줄일 수 있다.

[0082] 본 발명의 일측에 따른 이미지 스팸 필터링 방법은 기존 메일링 시스템을 새로 개발할 필요가 없이 각 포털 사이트의 메일 서버에 적용할 수 있다.

[0083] 본 발명의 일측에 따른 이미지 스팸 필터링 방법은 스마트 모바일 기기의 문자메시지 서비스, 모바일 메신저 서비스의 백그라운드 소프트웨어로 개발하여 쉽게 탑재 및 서비스 적용이 가능하다.

[0084] 본 발명의 일측에 따른 이미지 스팸 필터링 방법은 백신 프로그램에도 적용되어 이미지 스팸을 통해 배포되는 악성 소프트웨어 및 바이러스를 예방할 수 있다.

[0085] 실시예에 따른 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 실시예를 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic media), CD-ROM, DVD와 같은 광기록 매체(optical media), 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다. 상기된 하드웨어 장치는 실시예의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

[0086] 이상과 같이 실시예들이 비록 한정된 실시예와 도면에 의해 설명되었으나, 해당 기술분야에서 통상의 지식을 가진 자라면 상기의 기재로부터 다양한 수정 및 변형이 가능하다. 예를 들어, 설명된 기술들이 설명된 방법과 다른 순서로 수행되거나, 및/또는 설명된 시스템, 구조, 장치, 회로 등의 구성요소들이 설명된 방법과 다른 형태로 결합 또는 조합되거나, 다른 구성요소 또는 균등물에 의하여 대치되거나 치환되더라도 적절한 결과가 달성될 수 있다.

[0087] 그러므로, 다른 구현들, 다른 실시예들 및 특허청구범위와 균등한 것들도 후술하는 특허청구범위의 범위에 속한다.

부호의 설명

[0088] 110: 메시지 판단부

120: 이미지 변환부

130: LBP 추출부

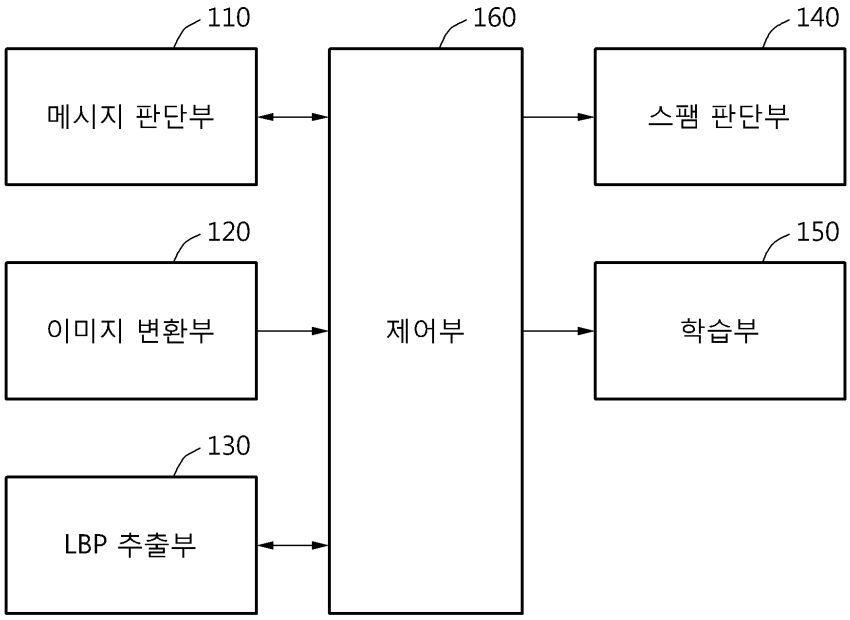
140: 스팸 판단부

150: 학습부

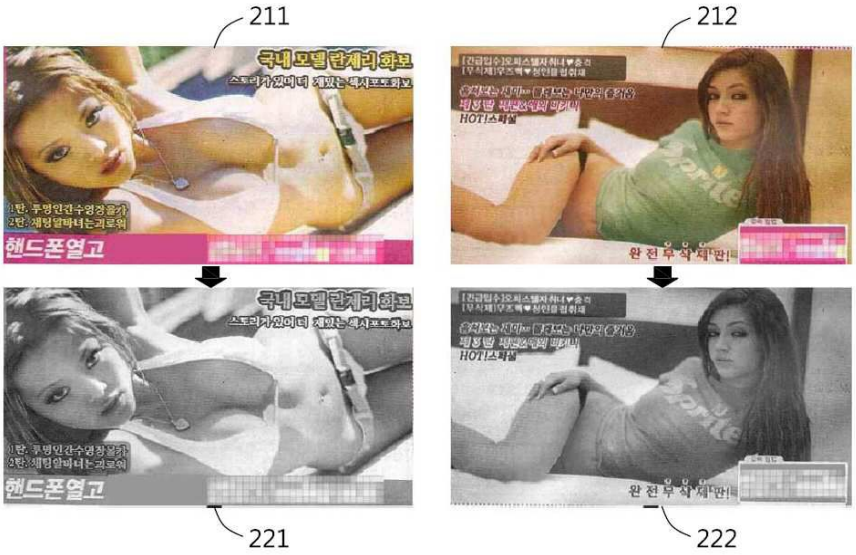
160: 제어부

도면

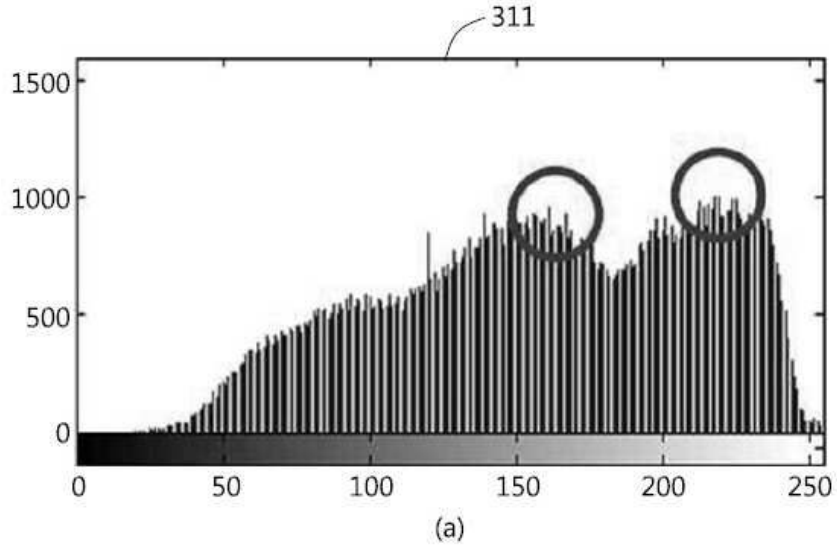
도면1


110
메시지 판단부
160
제어부
140
스팸 판단부
120
이미지 변환부
150
학습부
130
LBP 추출부

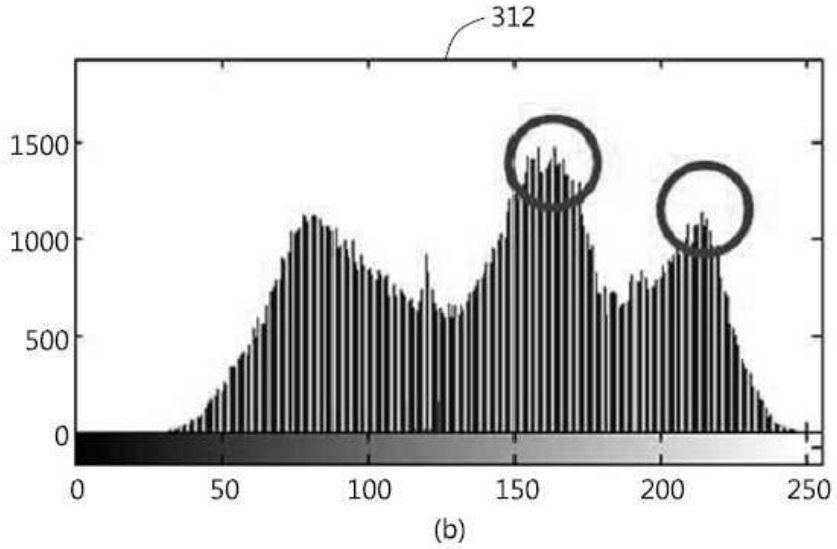
도면2


211
212
221
222

도면3

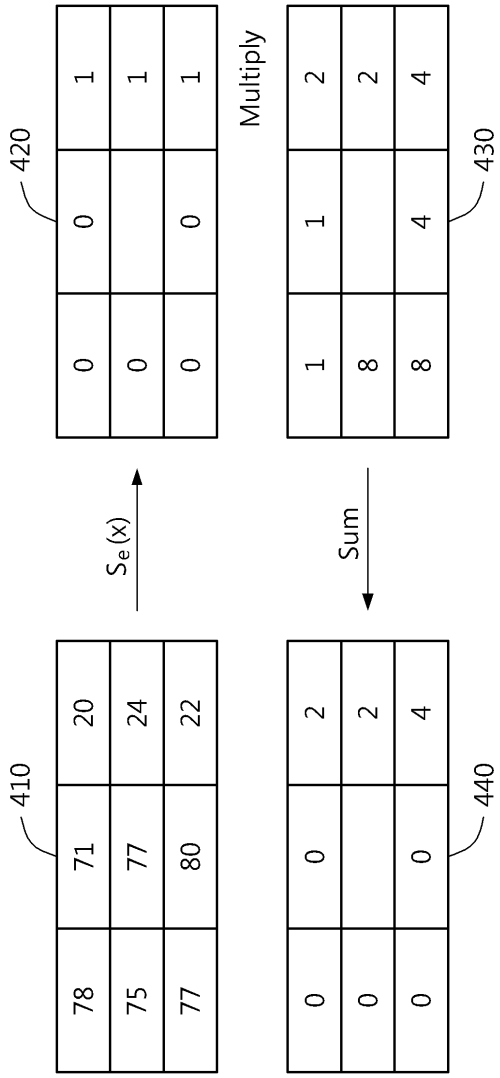

311
1500
1000
500
0
0
50
100
150
200
250

(a)

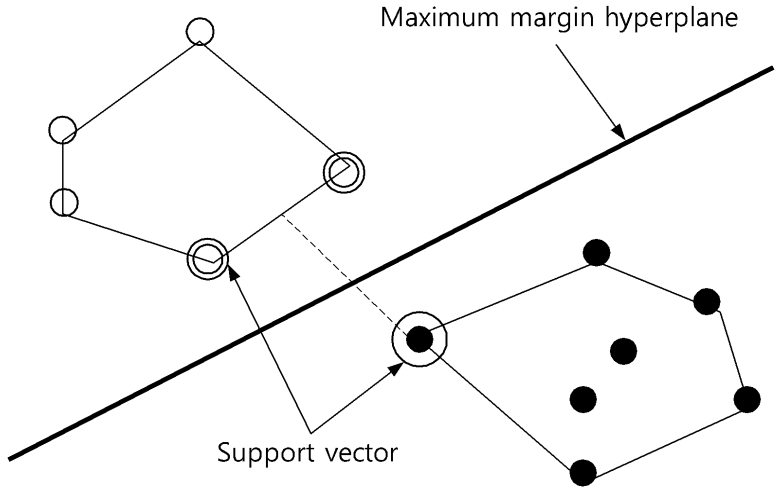

312
1500
1000
500
0
0
50
100
150
200
250

(b)

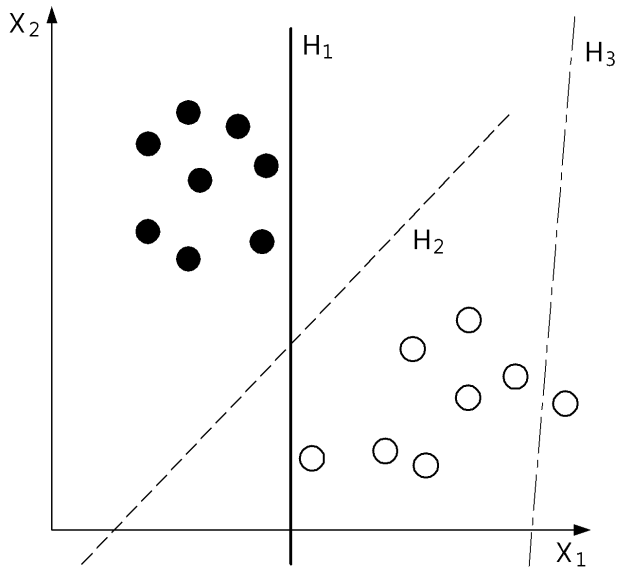
도면4


420
1 1 1
0 0
0 0 0
Multiply
2 2 4
1 4
1 8 8
430
Se(x)
Sum
410
20 24 22
71 77 80
78 75 77
2 2 4
0 0
0 0 0
440

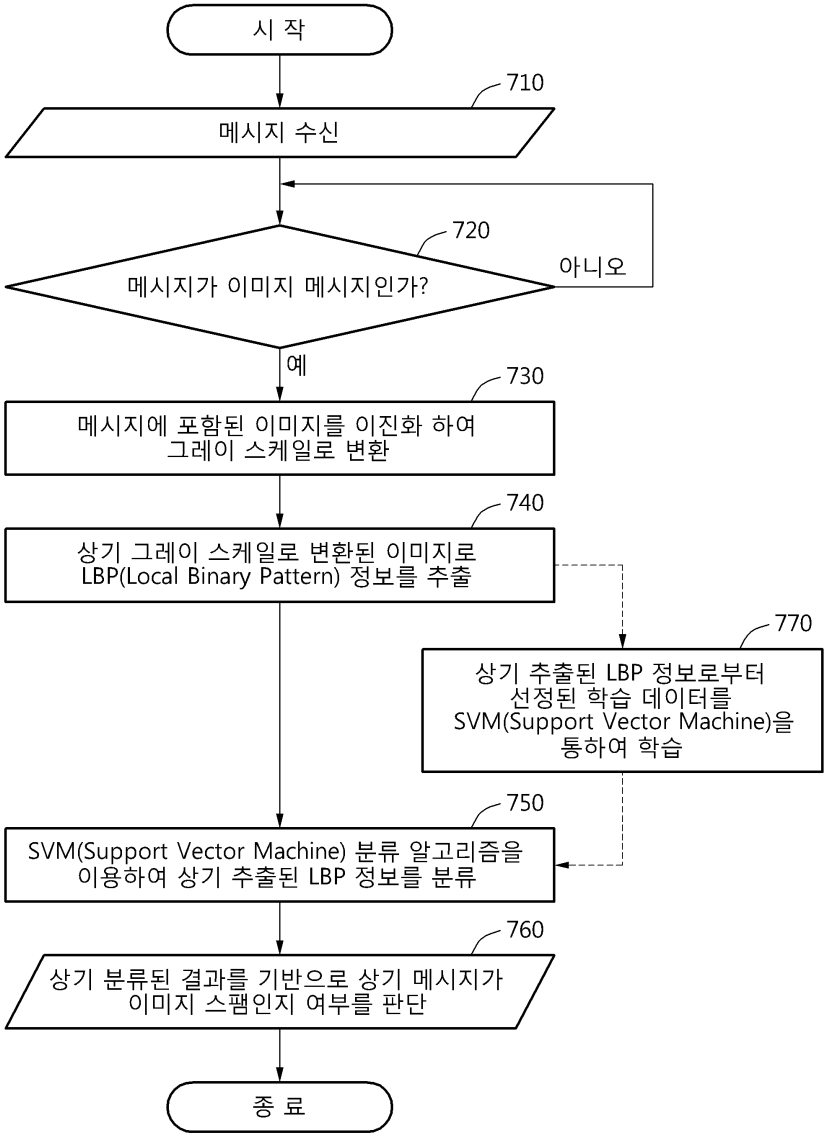
도면5


Maximum margin hyperplane
Support vector

도면6



도면7


시 작
710
메시지 수신
720
메시지가 이미지 메시지인가?
아니오
예
730
메시지에 포함된 이미지를 이진화 하여
그레이 스케일로 변환
740
상기 그레이 스케일로 변환된 이미지로
LBP(Local Binary Pattern) 정보를 추출
770
상기 추출된 LBP 정보로부터
선정된 학습 데이터를
SVM(Support Vector Machine)을
통하여 학습
750
SVM(Support Vector Machine) 분류 알고리즘을
이용하여 상기 추출된 LBP 정보를 분류
760
상기 분류된 결과를 기반으로 상기 메시지가
이미지 스팸인지 여부를 판단
종 료