**졸업논문 제안서**

**URL과 이미지 비교를 이용한 웹 사이트**

**위•변조 탐지 및 알림 서비스**

**Ver. 1.0**

**2019. 04. 02**

**한국외국어대학교 정보통신공학과**

**201403586 허성윤**

**201602119 유진솔**

지 도 교 수 : 정성호

**문서 정보**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 구 분 | 소 속 | 성 명 | 날 짜 | 서 명 |
| 작성자 | 한국외국어대학교 | 유진솔 | 2019. 04. 02 |  |
| 한국외국어대학교 | 허성윤 | 2019. 04. 02 |  |
| 검토자 | 한국외국어대학교 | 유진솔 | 2019. 04. 02 |  |
| 한국외국어대학교 | 허성윤 | 2019. 04. 02 |  |
| 승인자 | 한국외국어대학교 | 정성호 | 2019. 04. 02 |  |

**머리말**

본 문서는 URL과 이미지 비교를 이용한 웹사이트 위•변조 탐지 및 알림 서비스 소개와 연구 목적, 배경을 설명하고 관련 연구 분석과 함께 본 시스템을 구축하기 위한 시나리오를 기술한다.

**개정 이력**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **버전** | **작성자** | **개정일자** | **개정 내역** | **승인자** | |
| 1.0 | 허성윤 | 2019. 03. 31 | 초안 작성 |  | |
| 유진솔 |
| 검토자 | 허성윤, 유진솔 | | | |
| 1.1 | 허성윤 | 2019. 04. 01 | 초안 수정 |  | |
| 유진솔 |
| 검토자 | 허성윤, 유진솔 | | | |
| 1.2 | 허성윤 | 2019. 04. 01 | 최종 수정 | |  |
| 유진솔 |
| 검토자 | 허성윤, 유진솔 | | | |

목 차

목차

[목 차 5](#_Toc4945037)

[1. 서론 7](#_Toc4945038)

[1.1 서비스 정의 7](#_Toc4945039)

[1.2 서비스 기획 배경 및 목적 7](#_Toc4945040)

[1.2.1 웹사이트 위•변조 공격 – 피싱(Phishing)과 파밍(Pharming) 7](#_Toc4945041)

[1.2.2 웹사이트 위•변조 공격 – hosts파일 및 hosts.ics 파일 변조 8](#_Toc4945043)

[2. 관련 연구 조사 및 분석 9](#_Toc4945046)

[2.1 Feature Matching 기반 탐지 기법 9](#_Toc4945047)

[2.2 URL 기반 탐지 기법 9](#_Toc4945050)

[2.3 시각적 추출 기법(Visual Descriptor)과 SVM을 이용한 탐지 기법 10](#_Toc4945056)

[3. 주제 제안 10](#_Toc4945057)

[3.1 시나리오 10](#_Toc4945058)

[3.1.1 URL 일치 여부 확인 11](#_Toc4945060)

[3.1.2 Inception-v3를 이용한 이미지 유사도 검출 11](#_Toc4945061)

[3.1.3 dHash를 이용한 이미지 유사도 검출 11](#_Toc4945062)

[3.2 사용 기술 설명 12](#_Toc4945063)

[3.2.1 TensorFlow 12](#_Toc4945064)

[3.2.2 Transfer Learning 12](#_Toc4945066)

[3.2.3 dHash Algorithm 13](#_Toc4945067)

[4. 개발 일정 14](#_Toc4945068)

[5. 참고 문헌 15](#_Toc4945069)

1. 서론

1.1 서비스 정의

본 서비스는 URL과 이미지 비교를 이용하여 공공기관 및 금융기관 웹 사이트의 위•변조 여부를 탐지하여 사용자에게 알림 까지 제공하도록 응용 프로그램을 제공한다.

1.2 서비스 기획 배경 및 목적

온라인을 이용한 업무와 금융서비스의 보편화로 인하여, 사용자가 늘어남에 따라 정부나 금융기관 사이트를 모방해 개인•금융 정보를 노리는 해커들로부터 쉽게 노출되는 상황이 발생하게 되었다. 정부나 금융기관 사이트를 모방해 개인•금융 정보를 노리는 피싱(phishing: 개인정보를 빼내는 범죄) 사이트 차단 건수가 2017년 기준 처음 1만건을 넘어선 것으로 나타났다. 피싱 사이트는 금감원이나 은행 사이트와 똑같이 위장해 사용자들의 개인정보를 노린다.

한국인터넷진흥원(KISA)에 따르면 국내 웹사이트 변조 해킹이 2015년 615건, 2016년 1,056건(전년 대비 72%증가), 2017년 1,724건(전년 대비 63%증가)로 매넌 60% 이상 급증하고있는 추세이다. 이와 같은 웹사이트 위•변조 는 사용자가 사이트의 위•변조 여부를 직접 판단하기 어렵기 때문에 피해가 많이 발생하고 있는 실정이다.

이러한 웹사이트 위•변조 문제를 예방하기 URL과 웹사이트의 이미지를 이용하여 효율적으로 웹사이트를 탐지하고 예방할 수 있는 시스템을 제안한다.

1.2.1 웹사이트 위•변조 공격 – 피싱(Phishing)과 파밍(Pharming)

피싱(Phishing)은 개인정보(Private Data)와 낚시(Fishing)의 합성어로 웹사이트의 위장 홈페이지를 만든 뒤, 불특정 다수 이메일 사용자에게 메일을 발송하여 위장된 홈페이지로 접속하도록 현혹하여 개인정보를 빼내는 행위를 의미한다.

파밍(Phaming)은 피싱(Phishing)과 조작(Farming)의 합성어로 합법적으로 소유하고 있던 사용자의 도메인을 탈취하거나 DNS(Domain Name System) 이름을 속여서 사용자들이 진짜 사이트로 오인하도록 유도하는 해킹 방법이다.

[1]

PC가 파밍 악성 코드에 감염되면, 사용자는 정상 웹사이트에 접속을 했음에도 불구하고, 해커의 의해 변조된 임의의 가짜 사이트로 접속이 되어 개인정보 입력을 유도하게 된다.

1.2.2 웹사이트 위•변조 공격 – hosts 파일 및 hosts.ics 파일 변조

hosts 파일 변조는 사용자가 웹사이트에 접속하기 위해 URL을 입력하면 사용자 시스템의 ‘호스트’ 파일을 확인한다. 파일 내부에 입력된 영문 주소가 있으면 파일에 기록된 IP 주소로 웹사이트에 연결된다. 파일 내부에 영문 주소가 없으면 외부 네트워크에 있는 DNS 서버를 통해 변환된 IP 주소로 웹사이트에 연결된다. 호스트 파일이 변조되면 정상 URL을 입력해도 사용자가 모르는 사이 가짜 사이트로 연결된다.

[2]

[3]

호스트 파일을 변조한 웹사이트가 증가하고 호스트 파일 변조를 각종 보안 프로그램이 탐지하자, 공격자는 새로운 파일을 변조하게 됐다. 바로 hosts.ics 파일 변조이다. 웹사이트에 접속할 때 ‘hosts’ 파일보다 ‘hosts.ics’ 파일을 먼저 확인하게 된다.

따라서 보안 프로그램에 의해 변조 여부를 감시 받는 호스트 파일을 변조하지 않고, hosts.ics 파일을 변조하여 사용자를 가짜 사이트로 유도하는 것이다.

1. 관련 연구 조사 및 분석

2.1 Feature Matching 기반 탐지 기법



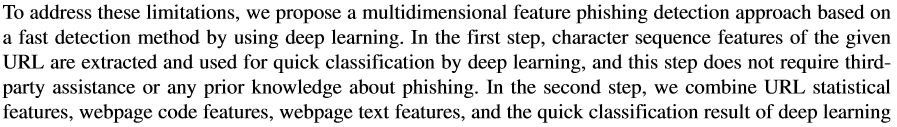
[4]

Feature Matching이란 수많은 Feature를 추출하여 다른 이미지의 Feature Set과 비교 후 유사성을 검사하는 OpenCV의 일종이다. 이미지에서 검출한 특성 포인트에 대해 색상을 지정해서 표시하고, 일치하는 특성 포인트를 하나의 선으로 연결한다. 특성 디스크립터의 개수를 줄이거나 늘임으로써 선의 개수를 조절할 수 있다. 하지만 선의 개수를 늘린다고 해도 이미지 전체에 대한 특성을 추출해내는 데에 한계가 있고, 그 특징을 추출하는 데에 시간이 상당히 소요되기 때문에 유사도 정확성과 효율이 떨어진다.

2.2 URL 기반 탐지 기법



[5]



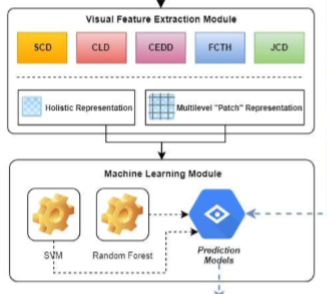
위 논문은 URL을 기반으로 위•변조 웹 사이트를 탐지한 연구이다. 이 연구에서는 URL 시퀀스

기능을 추출하여 Deep Learning을 통해 분류하는 로직으로, URL 통계 기능, 웹 페이지 코드 기능, 웹

페이지 텍스트 기능 및 Deep Learning 분류 결과를 이용한다. 그러나, 이는 단지 URL만 탐지에 사용하기 때문에 정상 도메인 주소를 가진 피싱 사이트 탐지에 부적합하다는 결점이 있다.

2.3 시각적 추출 기법(Visual Descriptor)과 SVM을 이용한 탐지 기법

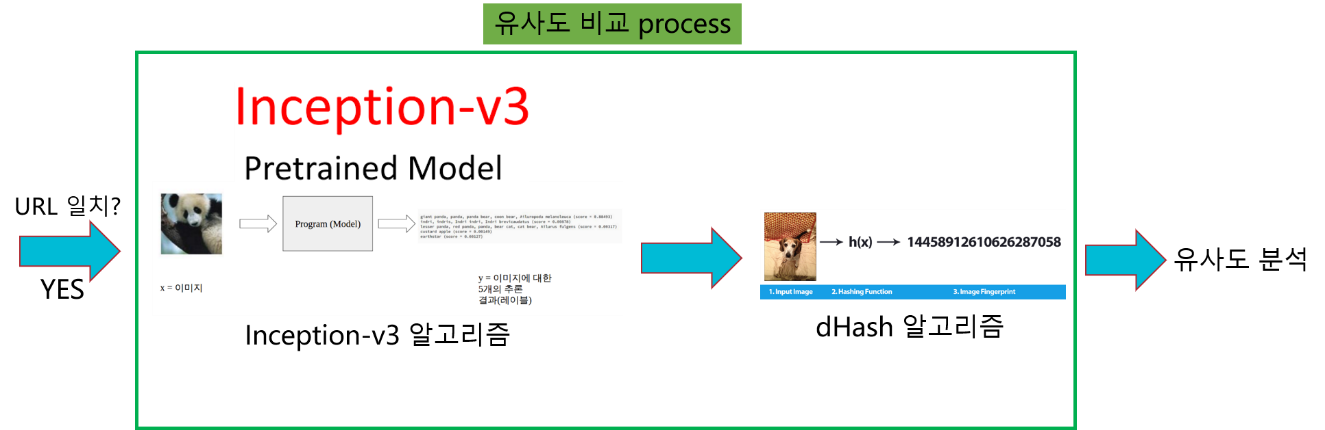


**[6]**

위 연구에서는 이미지의 특징을 추출하는 데에 Visual Descriptor를 사용해서 이미지의 색상이나 질감 등의 시각적 특징만을 추출해 낸다. 이후에 이미지를 분류하는 과정에 SVM을 사용한다. 하지만, Visual Descriptor는 이미 오래 전 기술이고 단순히 이미지의 시각적 특징만을 추출해 내기 때문에 다중 필터를 사용하는 Inception-v3의 성능이 더 우수하다고 판단하였다. 또한, 일반적으로 SVM은 본 연구에서 이용하는 Inception-v3에 비해 정확성이 떨어진다.

1. 주제 제안

3.1 시나리오



접속한 웹 페이지의 URL과 오리지널 URL의 일치 여부를 확인하고 일치 한다면, Inception-v3로 학습시켜 둔 모델에 비교 대상 이미지를 입력으로 넣어준다. 그렇게 해서 나온 결과 유사도 값과 dHash를 이용한 이미지 유사도를 분석하여 적당한 가중치를 준 뒤 이러한 과정을 적용하여 더 정확한 이미지 유사도를 검출하고자 한다.

3.1.1 URL 일치 여부 확인

* 1. 사용자의 URL을 입력받는다..
  2. python selenium으로 캡쳐한 웹 사이트 화면의 이미지 이름을 해당 URL로 저장한다.
  3. 이미지들의 이름, 즉 URL 리스트를 텍스트 파일로 생성한다.
  4. 사용자가 입력한 URL이 텍스트 파일에 있는 URL과 일치하는지 비교한다.
  5. 일치하지 않으면 변조사이트로 판단하고, 일치한다면 이미지 유사도 비교를 시작한다.

3.1.2 Inception-v3를 이용한 이미지 유사도 검출

1. 오리지널 사이트의 이미지 데이터 셋을 만든다.
2. 오리지널 사이트의 이미지를 사이트 별로 폴더로 분류하고 이 폴더를 데이터 셋으로 사용한다.
3. Inception V3를 사용하여 이미지 학습을 한다.
4. 오리지널 사이트의 데이터 셋을 input으로 넣어주고 이 이미지들을 (n, 299, 299 3)의 배열로 변환한다.
5. Convolution Layer와 Pooling Layer과정을 거쳐서 (n, 2048)의 배열로 변환한다.
6. Fully connected로 m개의 class로 분류한다.
7. Transfer Leaning을 위한 기존의 이미지 학습 모델의 오픈소스인 retrain.py를 이용하여 이미지 학습을 하여 Label을 생성한다.
8. 학습된 결과로 나온 Output Label과 사용자가 비교할 이미지와 비교하여 유사도를 검출한다.

3.1.3 dHash를 이용한 이미지 유사도 검출

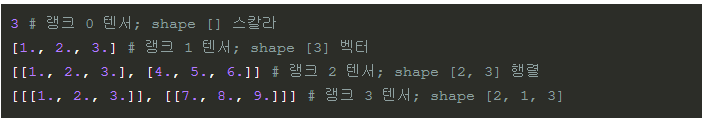
* 1. 오리지널 사이트의 이미지를 데이터베이스에 미리 저장해 둔다.

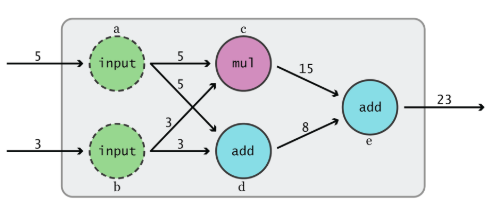
1. 웹 사이트에 접속하여 처음 보이는 홈 화면을 web application test framework의 일종인 selenium을 이용하여 캡쳐 후 로컬 파일에 자동 저장한다. (추가적인 비교를 위해 URL도 함께 저장한다.)
2. 웹 페이지의 유동적인 부분들로 인해 몇 분 간격으로 바뀌는 것까지 최대한 ‘같은 페이지의 많은 이미지’를 저장하기 위해 일정 시간 간격으로 캡쳐 하도록 한다.
   1. 오리지널 사이트의 이미지와 사용자가 접속한 사이트의 이미지를 비교하여 유사도를 검출한다.
3. Python에서 제공하는 libarary인 ImageHash에서 처리 속도가 빠르고 이미지 비교에 적합한 dHash 알고리즘을 사용한다.
4. 결과값으로 두 이미지의 차이 정도를 나타내는 해밍 거리 값을 얻는다.
   1. 검출된 유사도 정보로 사용자가 접속하고있는 사이트에 대한 유사도 정보를 제공한다.
5. 결과 해밍 거리 값을 가지고 오리지날과 유사한 정도를 백분율로 환산하여 100%라면 같은 이미지, 95%~99%라면 유사한 이미지, 그 이하라면 다른 이미지라고 판단한다.
6. 이 정보를 가지고 이 웹사이트의 위,변조 가능성을 경고하는 알림을 띄워준다.

3.2 사용 기술 설명

3.2.1 TensorFlow

텐서플로우는 데이터 흐름 그래프를 기반으로 하는 수치 계산을 위한 소프트웨어 프레임 워크이다. 텐서(tensor)는 Multidimensional Arrays라고 하며, 딥러닝 에서의 텐서는 다차원 배열로 나타내는 데이터를 의미한다. 랭크는 행렬들의 열들로 생성될 수 있는 백터 공간의 차원을 의미한다.

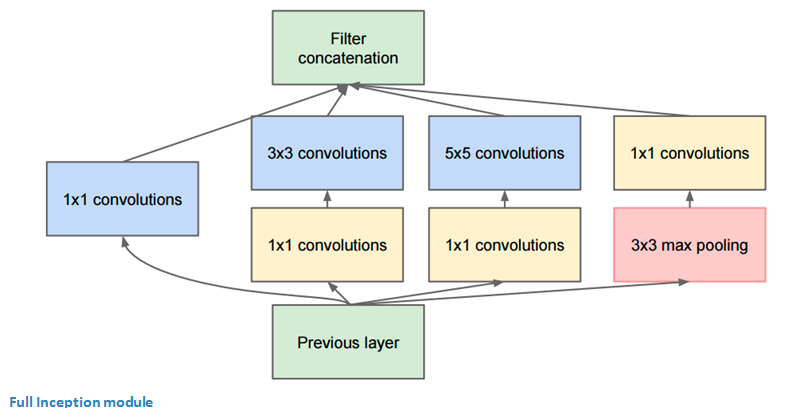
**[7]**

**[8]**

텐서는 노드(node)와 엣지(edge)로 구성된 Data Flow Graph를 통해 연산을 수행한다.

3.2.2 Transfer Learning

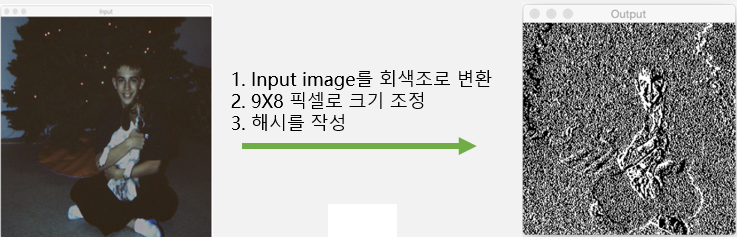
기존의 만들어진 모델을 사용하여 새로운 모델을 만들 시 학습을 빠르게 하며, 예측력을 높이는 방법이다.

**[9]**

Transfer Learning은 실질적으로 Convolution network을 처음부터 학습시키는 경우는 드물기 때문에, 이미 학습된 모델을 사용하여 문제를 해결하는데 이용한다.

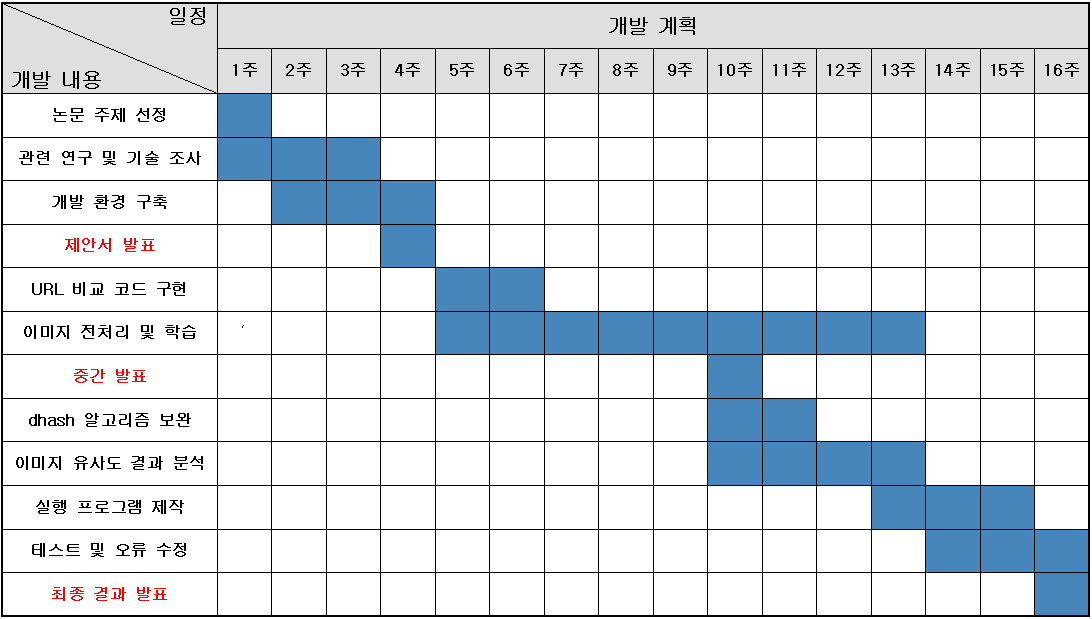
세부 조정(Fine-tuning)을 사용하여 기존 학습된 모델의 특징 추출과 다른 layer를 고정시키고 일부 layer만 조정하여 재 학습을 한다.

3.2.3 dHash Algorithm

**[10]**

dHash 알고리즘은 이미지의 인접 픽셀 간의 차이를 계산하여 만들어진 64비트 해시를 이용하여 해밍 거리를 구하고, 해밍 거리 값으로 이미지 유사도를 결정하는 방법이다.

1. 입력이미지를 회색조로 변환한다.
2. 이미지 크기 조정을 9 x 8 픽셀 나노로 크기 조정을 하여, 결과 이미지 해시가 초기 공간 크기에 관계없이 비슷한 사진과 크기가 일치 하도록 한다.
3. 인접한 픽셀의 차이를 계산하면 8가지 차이가 생겨서 8x8의 64비트 해시가 되고, 이 비트를 할당하여 해시를 작성한다.
4. 서로 다른 두 해시의 비트를 비교하여 해밍거리를 구한다.
5. 해밍거리가 0이면 두 해시가 동일하다, 즉 두 이미지가 동일하다는 것을 의미한다.
6. 개발 일정



1. 참고 문헌

[1]-<https://m.post.naver.com/viewer/postView.nhn?volumeNo=16585222&memberNo=25598567>

[2],[3] - <https://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?seq=23390>

[4]-https://www.earticle.net/Article/A263848 – 이미지를 이용한 웹사이트 위•변조 탐지

[5]-PENG YANG, GUANGZHEN ZHAO , AND PENG ZENG, “Phishing Website Detection Based on Multidimensional Features Driven by Deep Learning”, **Published in:**[IEEE Access](https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=6287639) ( Volume: 7 ), 11 January 2019

[6]-F.C. Dalgic1, A.S. Bozkir 2\* and M. Aydos 3, “Phish-IRIS: A New Approach for Vision Based Brand Prediction of Phishing Web Pages via Compact Visual Descriptors”, **Published in:**[2018 2nd International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT)](https://ieeexplore.ieee.org/xpl/mostRecentIssue.jsp?punumber=8543123), 19-21 Oct. 2018

[7]-http://solarisailab.com/archives/2351

[8]-<https://yamerong.tistory.com/40>

[9]-https://jsideas.net/Inception\_v3\_transfer\_learning/

[10]-https://www.pyimagesearch.com/2017/11/27/image-hashing-opencv-python/

**GitHub URL-https://github.com/yjinsol/grad\_project.git**