KIPS Trans. Comp. and Comm. Sys. 높은 정확도를 위한 이미지 전처리와 앙상블 기법을 결합한 이미지 기반 악성코드 분류 시스템에 관한 연구 225
Vol.11, No.7 pp.225~232 https://doi.org/10.3745/KTCCS.2022.11.7.225
ISSN: 2287-5891 (Print), ISSN 2734-049X (Online)

A Study on the Image-Based Malware Classification System that Combines Image Preprocessing and Ensemble Techniques for High Accuracy

Kim Hae Soo† · Kim Mi Hui††

ABSTRACT

Recent development in information and communication technology has been beneficial to many, but at the same time, malicious attack attempts are also increasing through vulnerabilities in new programs. Among malicious attacks, malware operate in various ways and is distributed to people in new ways every time, and to solve this malware, it is necessary to quickly analyze and provide defense techniques. If new malware can be classified into the same type of malware, malware has similar behavioral characteristics, so they can provide defense techniques for new malware using analyzed malware. Therefore, there is a need for a solution to this because the method of accurately and quickly classifying malware and the number of data may not be uniform for each family of analyzed malware. This paper proposes a system that combines image preprocessing and ensemble techniques to increase accuracy in imbalanced data.

Keywords : Malware, Deep Learning, Image Preprocessing, Ensemble

높은 정확도를 위한 이미지 전처리와 앙상블 기법을 결합한 이미지 기반 악성코드 분류 시스템에 관한 연구

김 해 수† · 김 미 희††

요 약

최근 정보통신 기술의 발전이 많은 이에게 이점이 되고 있지만, 그와 동시에 새로운 프로그램의 취약점을 통해 악의적 공격 시도 또한 증가하고 있다. 악의적 공격 중 악성코드는 다양한 방식으로 동작하며 매번 새로운 방식으로 사람들에게 유포되고 이러한 악성코드들을 해결하기 위해 발견된 악성코드를 빠르게 분석하여 방어기법을 제공해야 한다. 새로운 악성코드를 기존 악성코드와 동일한 종류로 분류할 수 있다면 동작의 유사성을 가진 악성코드들의 분석된 특징을 이용해 새로운 악성코드의 방어기법을 제공할 수 있다. 따라서 악성코드를 정확하고 빠르게 분류하는 방법이 있어야 한다. 또한, 분석된 악성코드들의 패밀리 마다 데이터의 개수가 균일하지 않을 수 있으므로 이에 대한 해결방안이 필요하다. 본 논문에서는 이미지 전처리 기법과 앙상블 기법을 결합하여 개수가 균일하지 않은 데이터에서 정확도를 높이는 시스템을 제안한다.

키워드 : 악성코드, 딥러닝, 이미지 전처리, 앙상블

1. 서 론

정보통신 기술의 발전을 통해 새로운 운영체제, 프로그램 등이 개발이 되어 우리에게 이점을 주었지만 취약점을 이용한 악의적인 공격으로 많은 이들에게 피해를 주고 있다[1].

많은 악의적인 공격 중 악성코드는 다양한 방식으로 동작하고 매번 새로운 방식으로 사람들에게 유포된다. 새로운 악성코드는 계속해서 발견되고 있고 그와 동시에 악성코드의 수가 빠르게 증가하고 있다. 기존 악성코드의 시그니처 비교를 통한 분석, 분류로는 모든 악성코드를 관리할 수 없고 새로운 악성코드가 생길 때마다 분석하고 방어기법을 찾는 방식으로는 증가하는 악성코드의 수를 따라잡을 수 없으며 분석이 끝나기 전에 새로운 악성코드가 발견될 가능성이 생긴다[2]. 2021년 6월 WatchGuard Technologies의 조사 결과에 따르면 기존 방식으로 탐지에 실패한 악성코드가 74%에 달한다[3]. 따라서 새로운 악성코드를 대응하기 위해 빠르게 악성코드를 분석, 분류할 방법을 찾아야 한다.

동일한 종류의 악성코드들은 동작의 유사성을 갖고 있고 기존의 악성코드의 패밀리로 분류를 할 수 있다면 분석된 악성코드를 이용해 새로운 악성코드의 유형을 알아낼 수 있고

※ 이 논문은 2018년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No.2018R1A2B6009620).
† 준 회 원 : 한경대학교 컴퓨터응용수학부 석사과정
†† 종신회원 : 한경대학교 컴퓨터응용수학부 컴퓨터시스템연구소 교수
Manuscript Received : February 7, 2022
Accepted : March 11, 2022
* Corresponding Author : Kim Mi Hui(mhkim@hknu.ac.kr)

적절한 방어기법을 제공할 수 있을 것이다.

악성코드들의 특성을 학습한 인공지능을 이용하면 유사한 특성을 가진 악성코드들을 빠르게 분류해낼 수 있다.

이를 위해 이미지 기반 분류기법[4]이 제안되었으나 높은 정확도를 제공하지 못했고, 데이터의 클래스 불균형 상황, 즉 악성코드 패밀리 별의 데이터 개수가 균일하지 않은 것을 고려하지 않아 이를 해결하는 방안도 필요하다.

이에 [5]에서는 새로운 악성코드를 빠르게 분석하고 방어하기 위해 악성코드의 바이너리 파일을 시각화하여 CNN (Convolutional Neural Networks) 모델을 통해 분류하는 시스템을 제안하였다. 또한 정확도를 높이기 위해 LBP(Local Binary Pattern), HOG(Histogram of Oriented Gradients)를 통해 악성코드 이미지에서 중요한 특성을 찾고 데이터 클래스 불균형에서 오는 문제를 CNN 모델들의 앙상블 모델을 통해 해결하였다. 본 논문의 기여는 다음과 같다.

- [5]에서 제안한 시스템을 상세히 제안
- [5]의 실험 결과에 LBP, HOG와 다양한 데이터를 사용하여 성능 실험 분석

본 논문은 2장에서는 이미지 기반 악성코드에 대한 관련연구를 소개하고, 3장에서는 제안 시스템의 구조를 자세하게 설명한다. 4장에서는 성능 평가 방법의 설명 및 각 기법(특성 추출, 앙상블 기법)에 대해 성능을 평가하고 5장에서 결론을 맺는다.

2. 관련 연구

2.1 이미지 기반 악성코드 연구

딥러닝을 이용한 악성코드 탐지와 분류에 관한 연구는 여러 가지 방법으로 이루어지고 있다[6]. 이미지 기반 악성코드 탐지에서 [7]의 연구에서는 Linux 악성코드들을 64x64 크기로 시각화하고 LBP, Median Filter와 같은 영상처리 기법과 Hard voting을 통해 악성코드를 탐지하는 시스템을 구성했으며 각각 영상처리 기법을 적용하지 않은 Original에서 98.77% LBP는 96.47% Median Filter에서는 98.57%의 정확도를 도출해냈고 세 가지 영상처리 기법을 적용한 모델들로 Hard voting classification을 이용했을 때의 정확도는 98.87%로 상승한 것을 볼 수 있다.

탐지뿐만 아니라 악성코드 분류기법 중 데이터 클래스 불균형을 해결하기 위한 [8]의 연구에서는 클래스별로 측정되는 Softmax loss값에 해당 클래스의 가중치 값을 계산해서 곱한 Weighted Softmax loss값을 이용한 것을 사전학습 모델의 마지막 계층에 추가하여 실험을 진행했다. 모델에 따라 정확도 측면에서 부족한 점이 있고 해당 기법은 새로운 기존 모델에 Weighted Softmax Loss 레이어를 추가해야 하는 단점이 있다.

본 논문에서는 기존의 모델을 그대로 사용하면서 영상처리 기법, 즉 LBP, HOG를 이용한 이미지 전처리와 기존 모델을 여러 개 사용하여 여러 모델이 출력한 결과를 통합해 분류하는 Soft Voting 앙상블 기법을 적용해 악성코드 분류를 진행한다.

3. 제안 시스템

본 장에서는 본 논문에서 제안하는 이미지 기반 악성코드 분류 시스템을 설명한다. Fig. 1은 제안 시스템의 구조를 나타내며, 제안 시스템은 이미지 생성 모듈(Image Generation Module, IGM), 특성 선택 모듈(Feature Selection Module, FSM), 악성코드 분류 모듈(Malware Classification Module, MCM)로 구성된다. 악성코드 바이트 파일이 IGM의 입력이 되며 데이터 변환 과정 후 회색조 이미지가 출력된다. 회색조 이미지는 FSM을 통해 전처리를 진행하고 전처리된 이미지는 MCM을 통해 학습하고 분류한다.

3.1 이미지 생성 모듈(IGM)

IGM은 바이너리 형태로 이루어진 악성코드를 1Byte 단위로 나누어서 2차원 배열의 형태로 구성하고 해당 배열을 정해진 너비를 기준으로 회색조 이미지로 만든다. Table 1은 이미지의 너비를 정하는 기준이다[4].

Fig. 2는 16진수 형태로 이루어진 악성코드의 예이며 이 악성코드를 1바이트 단위로 10진수로 변환하고 배열로 만들고 변환된 배열을 이미지 형태로 만든 것이 Fig. 3이다.

3.2 이미지 특성 선택 모듈(FSM)

FSM은 3.1장에서 설명한 IGM에서 생성한 이미지를 선택된 특성에 따라 전처리를 해주는 모듈이다. RAW는 생성된 이미지를 전처리하지 않고, LBP, HOG를 선택하면 선택한 방식으로 이미지 특징추출 작업을 한다.

1) LBP

LBP는 모든 픽셀을 대상으로 주변 3x3 크기의 영역에서 중심 픽셀을 기준으로 상대적인 밝기의 크기를 2진수로 계산하는 알고리즘으로 동작한다[9]. Fig. 4에서 Fig. 4A는 이미지 한 부분의 예시이고, Fig. 4B는 중심 픽셀을 기준으로 크거나 같으면 1 작으면 0으로 대치하여 Fig. 4C처럼 8자리의 이진수로 변환한다. 최종적으로 이진수 값을 십진수로 다시 변환하여 중심 픽셀의 값은 Fig. 4D와 같이 된다. Fig. 5는 Fig. 3을 위의 과정으로 만든 그림이다.

본 논문에서는 동일한 종류의 악성코드 이미지의 유사성은 유사한 텍스쳐를 갖고 있을 것이라 보고 LBP를 적용하였다.

2) HOG

HOG는 일정 영역의 크기를 셀로 분할 한 후 각 셀의 엣지(Edge) 정보를 특징으로 추출하는 알고리즘으로 동작한다[10]. Fig. 6은 HOG를 통해 만들어진 그림이다.

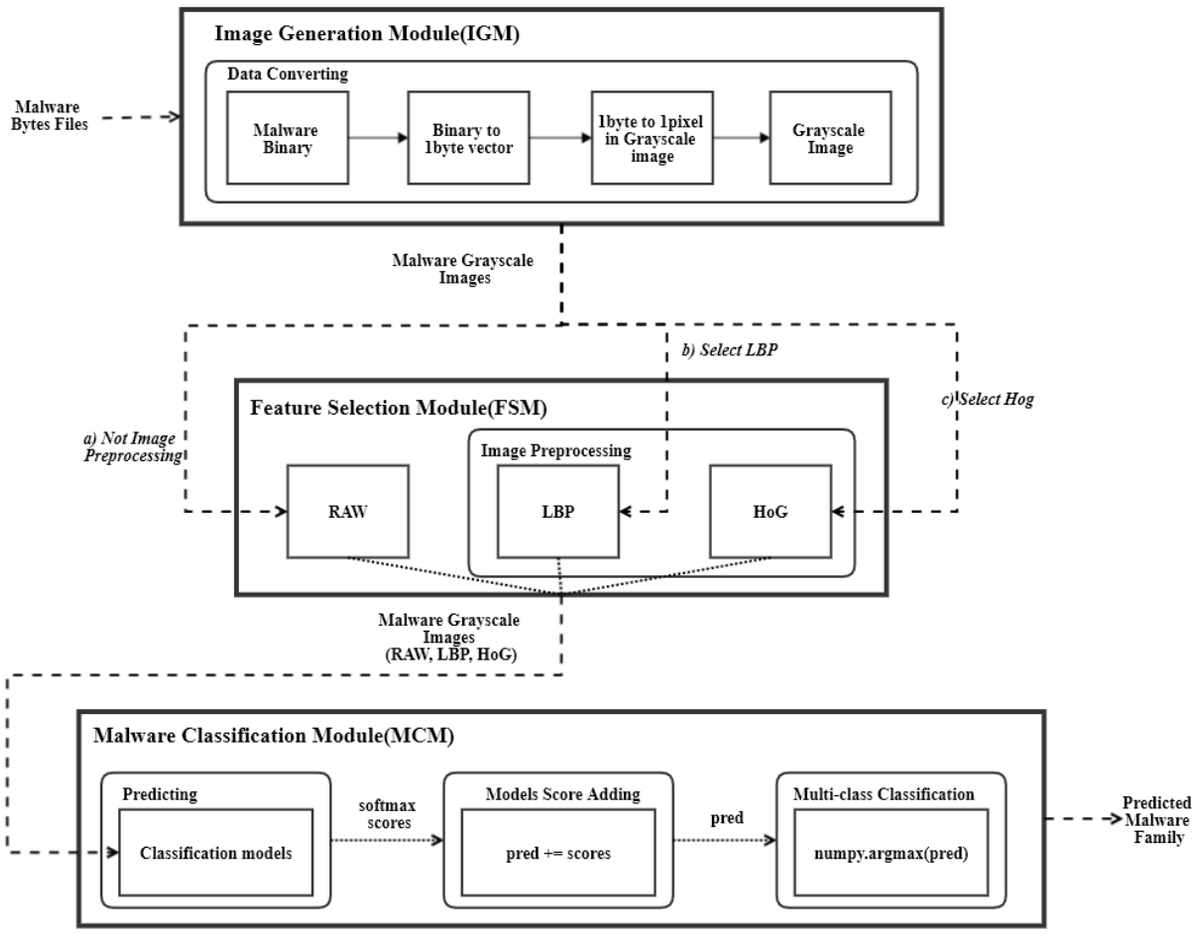


Fig. 1. Proposal System

Table 1. Image Width for Various File Sizes[4]

File Size Range	Image Width
〈 10kB	32
10kB~20kB	64
20kB~60kB	128
60kB~100kB	256
100kB~200kB	384
200kB~500kB	512
500kB~1000kB	768
1000kB 〈	1024

본 논문에서는 동일한 종류의 악성코드 이미지의 유사성은 각 이미지에서 추출되는 엣지 정보가 유사할 것이라 보고 HOG를 적용하였다.

3.3 악성코드 분류 모듈(MCM)

MCM은 3.2장에서 선택된 특성에 따라 처리된 이미지를 학습한 분류모델들을 이용해 악성코드의 패밀리를 예측한다.

```
FF 25 F8 80 00 10 FF 25 F4 80 00 10 FF 25 D8 80
00 10 FF 25 E8 80 00 10 55 8B EC 83 EC 10 A1 00
90 00 10 83 65 F8 00 83 65 FC 00 53 57 BF 4E E6
```

Fig. 2. Example of Malware Byte File

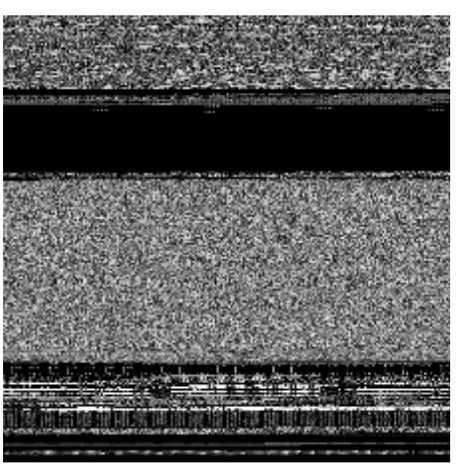
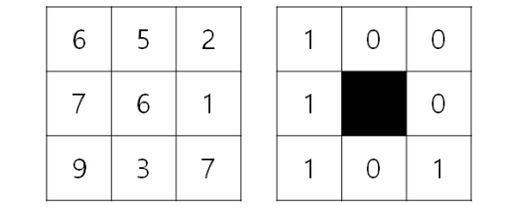
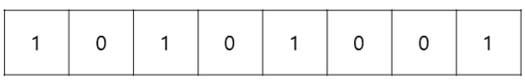


Fig. 3. Malware Image : Ramnit



(Fig. 4A) (Fig. 4B)



(Fig. 4C)

(Fig. 4D)

Fig. 4. Process of Convert`ing LBP[9]

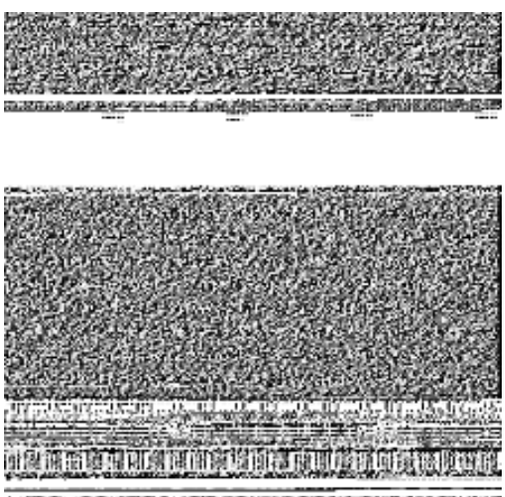


Fig. 5. Image Converted Into LBP : Ramnit

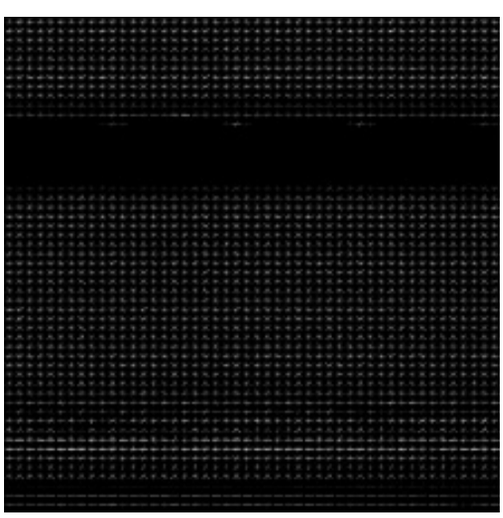


Fig. 6. Image Converted Into HOG : Ramnit

1) CNN[11]

이미지 기반 악성코드 분류를 위해 기본적인 학습 모델로 CNN을 사용한다.

Table 2는 본 논문에서 사용한 CNN모델의 구조도이다. 4개의 Convolution Layer와 Convolution Layer들 사이에 2 × 2 크기의 Maxpooling Layer를 추가해 Convolution Layer의 filter들에 의해 무수하게 많이 늘어난 특징의 수를 조절하고 0.5의 확률로 일부 뉴런을 생략하여 학습을 진행하는 Dropout Layer를 Convolution Layer와 Dense Layer사이에 배치해 Convolution Layer에서 추출한 특징을 일부만 Dense Layer에 전달한다. 마지막 Dense Layer의 units은 분류하려는 클래스의 개수이다.

2) LSTM(Long Short-Term Memory)[12]

앙상블 기법을 위해 추가한 모델로 악성코드의 데이터가 순차적으로 이루어져 있는 시계열 데이터라는 점을 이용해서 LSTM 알고리즘을 사용한다. LSTM은 시그모이드와 tanh를

Table 2. Structure of CNN model

Layer	parameters	values	output
Input Layer		224×224	224×224×1
Convolution Layer_1	filter	32	224×224×32
	kernel_size	3×3	
	strides	1	
Convolution Layer_2	filter	128	224×224×128
	kernel_size	3×3	
	strides	1	
Max Pooling Layer_1	pool_size	2×2	112×112×128
Convolution Layer_3	filter	128	112×112×128
	kernel_size	3×3	
	strides	1	
Max Pooling Layer_2	pool_size	2×2	56×56×128
Convolution Layer_4	filter	256	56×56×256
	kernel_size	3×3	
	strides	1	
Dropout Layer	rate	0.5	56×56×256
Max Pooling Layer_1	pool_size	2×2	28×28×256
Flatten Layer			200,704
Dense Layer	units	512	512
	activation	‘relu’	
Dense Layer	units	256	256
	activation	‘relu’	
Dense Layer	units	n_classes	n_classes
	activation	‘softmax’	

결합한 세 개의 레이어로 이전상태와 현재 상태를 계속해서 업데이트하며 정보를 유지해나가는 알고리즘으로 동작하여 시계열 데이터 예측에 효과적이다.

3) 앙상블 기법

딥러닝에서 조심해야 하는 것 중 하나가 데이터 클래스 불균형이다[13]. 데이터 클래스 불균형이란 데이터 셋에서 각 클래스 간의 데이터 개수 차이가 큰 경우를 말한다[14]. 데이터 개수가 적은 클래스는 모델의 레이어들이 해당 클래스의 특징을 제대로 학습하지 못해 모델이 분류할 때 제대로 된 결과를 출력해내지 못한다. 이러한 클래스 불균형을 해결하기 위해 두 개 이상의 모델이 도출해낸 결과들을 이용하여 최종적인 분류를 해내는 앙상블 기법이 있다.

본 논문에서 다수결 분류 방식의 앙상블 기법을 이용한다. 다수결 분류에는 모델이 가장 많이 선택한 클래스로 분류가 되는 Hard Voting이 있고 모델이 출력한 값들을 모두 더해서 가장 큰 값을 가진 클래스로 분류하는 Soft Voting이 있으며 본 논문에서는 Soft Voting 방법으로 분류한다.

4. 성능 평가

본 장에서는 제안 시스템을 성능 평가하기 위한 실험환경을 설명하고 실험 결과를 분석한다.

4.1 실험 환경

실험은 Intel core i7-10700F CPU, 16GB RAM, Geforce RTX 2080 SUPER GPU 환경에서 진행하며 파이썬 3.8.10 버전의 텐서플로우 2.5.0버전을 통해 모델을 구성한다.

1) 실험 데이터

본 논문에서 실험에 이용한 데이터는 Kaggle에서 제공하고 있는 BIG 2015 (Microsoft Malware Classification challenge)[15] 데이터와 Malimg[4] 데이터이다.

Table 3에 표기된 샘플의 개수를 보면 패밀리 중에 가장 많은 데이터 수는 2942개이고 가장 적은 데이터 수는 42개이다. Table 4의 가장 많은 데이터 수는 2949개이고 가장 적은 데이터 수는 80개 이지만 대부분의 클래스가 가장 많은 데이터를 가진 클래스와 개수 차이가 크다.

실제 데이터는 클래스 간 데이터의 수가 비슷하지 않을 것이기 때문에 이처럼 클래스 별 데이터 수의 차이가 큰 데이터를 이용해서 제안 모델의 성능을 측정한다.

2) 성능 평가 방법

본 논문에서는 기본 이미지(즉, RAW), 두 가지 전처리 방법(즉, LBP, HOG)과 CNN모델에 앙상블 기법이 적용된 모델들을 통해 전처리와 앙상블이 정확도 개선에 얼마나 효과적인지 실험하여 평가한다.

Table 3. BIG 2015 Dataset[15]

#	Familly name	#Train Sample	Type
1	Rammit	1541	Worm
2	Lollipop	2478	Adware
3	Kelihos_ver3	2942	Backdoor
4	Vundo	475	Trojan
5	Simda	42	Backdoor
6	Tracur	751	TrojanDownloader
7	Kelihos_ver1	398	Backdoor
8	Obfuscator.ACY	1228	Any kind of obfuscated malware
9	Gatak	1013	Backdoor

Table 4. Malimg Malware Dataset[4]

#	Family name	#Train Sample	Type
1	Allaple.L	1591	Worm
2	Allaple.A	2949	Worm
3	Yuner.A	800	Worm
4	lolyda.AA 1	213	PWS
5	lolyda.AA 2	184	PWS
6	lolyda.AA 3	123	PWS
7	C2Lop.P	146	Trojan
8	C2Lop.gen!G	200	Trojan
9	Instantaccess	431	Dialer
10	Swizzor.gen!I	132	Trojan Downloader
11	Swizzor.gen!E	128	Trojan Downloader
12	VB.AT	408	Worm
13	Fakerean	381	Rogue
14	Alueron.gen!J	198	Trojan
15	Malex.gen!J	136	Trojan
16	Lolyda.AT	159	PWS
17	Adialer.C	125	Dialer
18	Wintrim.BX	97	Trojan Downloader
19	Dialplatform.B	177	Dialer
20	Dontovo.A	162	Trojan Downloader
21	Obfuscator.AD	142	Trojan Downloader
22	Agent.FYI	116	Backdoor
23	Autorun.K	106	Worm:AutoIT
24	Rbot!gen	158	Backdoor
25	Skintrim.N	80	Trojan

평가 방법은 결과로 출력된 softmax값과 onehot encoding 방식으로 인출된 label값을 비교해서 boolean값을 인출하고 True를 1.0, False를 0.0으로 변환 후 모든 결과에 대해 평균을 구하고 해당 값을 정확도로 하여 모델의 성능을 측정 및

각 전처리 방법 및 모델별 정확도를 비교한다.

또한, 각 클래스 정확도를 측정해 적은 수의 데이터를 가진 클래스의 정확도 상승률이 어느 정도인지 분석한다.

4.2 실험 결과 분석

1) 특성 추출 기법

본 절에서는 각 특성 추출 기법에 따른 정확도를 확인하고 분석한다. Fig. 7과 Fig. 8은 BIG 2015 데이터 Table 3와 Malimg 데이터 Table 4의 정확도 차이를 보여주는 막대 그래프이다.

Table 5은 BIG 2015 데이터의 정확도를 정리한 것이다. Table 5에서 보이는 것처럼 LBP는 RAW의 정확도에 비해 CNN 단일모델에서 0.69%, 앙상블 CNN 모델에서는 0.13%, 앙상블 CNN LSTM 모델에서 0.14%상승하였다. HOG는 정확도가 각각 1.25%, 0.33%, 1.06% 감소하였다.

Table 6은 Malimg 데이터의 정확도를 정리한 것이다. Table 6에서 보이는 것처럼 정확도가 각각 LBP는 0.38%, 0.27% 증가하였고 CNN LSTM 앙상블 모델에서 0.19% 감소하였다. HOG는 정확도가 각각 0.27%, 0.59%, 2.26% 감소하였다.

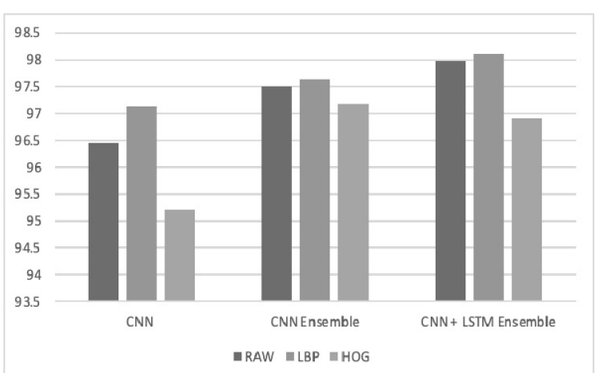


Fig. 7. Accuracy by Data Preprocessing Method and Model : BIG 2015

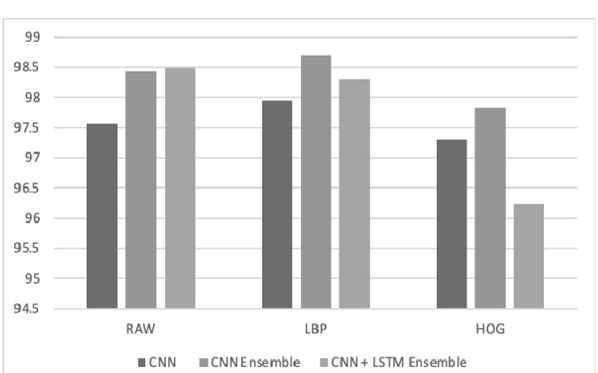


Fig. 8. Accuracy by Data Preprocessing Method and Model : Malimg

Table 5. BIG 2015 Experiment Results Accuracy Table

Accuracy (%)	CNN	CNN Ensemble	CNN and LSTM Ensemble
RAW	96.45	97.51	97.97
LBP	97.14	97.64	98.11
HOG	95.2	97.18	96.91

Table 6. Malimg Experiment Results Accuracy Table

Accuracy (%)	CNN	CNN Ensemble	CNN and LSTM Ensemble
RAW	97.57	98.43	98.49
LBP	97.95	98.7	98.3
HOG	97.3	97.84	96.23

지금까지의 결과를 종합해보면, 악성코드 이미지에서 추출되는 악성코드 이미지의 엣지 정보를 시각화한 것(HOG) 보다 텍스쳐 정보를 시각화한 것(LBP)이 악성코드 분류에 있어 더 효과적인 특성임을 나타낸다.

2) 앙상블 기법

본 절에서는 앙상블 기법에 따른 정확도를 분석한다.

Fig. 9는 BIG 2015 데이터의 특성 추출 기법들을 통해 도출된 클래스별 정확도를 앙상블 기법에 따라 평균을 낸 것이다.

앙상블 모델들의 정확도가 대부분의 클래스에서 단일 모델보다 더 높은 정확도를 보이며, 특히 데이터의 개수가 적었던 Simda에서 41.67%에서 62.5%로 20.83%라는 눈에 띄는 정확도 상승률을 보였다. 이외에도 대부분의 클래스에서 정확도가 상승하여 단일모델 평균 89.3%에서 CNN 앙상블로 93.04%, CNN LSTM 앙상블은 93.21% 상승하였다.

Fig. 10은 Malimg 데이터의 데이터 특성 추출 기법들을 통해 도출된 클래스별 정확도를 앙상블 기법에 따라 평균을 낸 것이다.

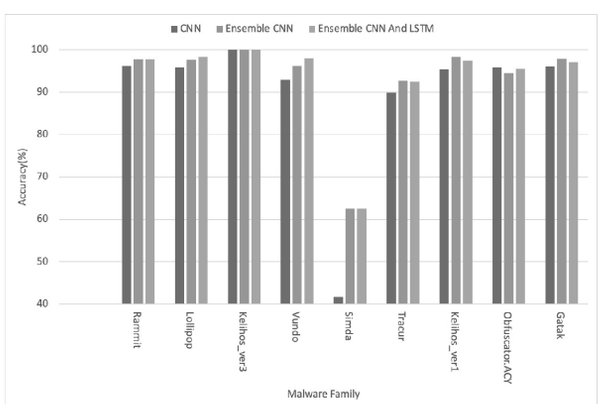


Fig. 9. Accuracy of BIG 2015 Data by Ensemble Techniques

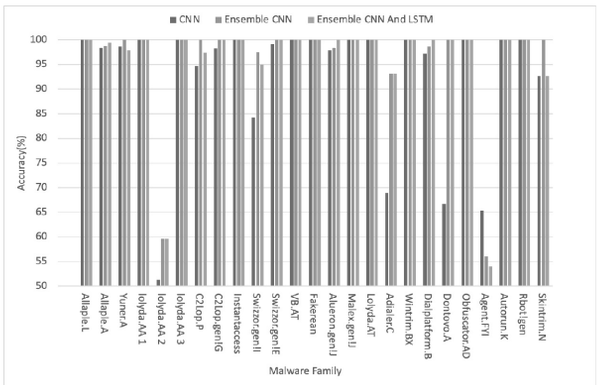


Fig. 10. Accuracy Average of Malimg Data by Ensemble Techniques

lolyda.AA 2가 8.34% 상승했고 Swizzor.gen!I가 13.33%, Adialer.C가 24.15%, Dontovo.A가 33.33% 상승하였다. 전체 단일모델 평균 92.53%에서 CNN 앙상블이 96.08%로 상승하였고, CNN LSTM 앙상블이 95.56%로 상승하여 단일모델보다 앙상블 모델이 정확도가 더 상승한 것을 알 수 있다.

BIG 2015 데이터는 하나의 클래스가 적은 개수의 데이터를 갖고 있었고 해당 클래스의 정확도가 모든 부분에서 개선되는 경향을 보여주었다. Malimg 데이터는 많은 클래스가 적은 수의 데이터를 갖고 있다. RAW 이미지는 다른 처리를 하지 않았기 때문에 정확도가 증가하였고 LBP는 CNN 단일모델에서는 RAW 이미지의 결과보다 더 나은 성능을 보였다. 그러나 LSTM에서는 LBP 알고리즘의 특성상 RAW 이미지의 텍스쳐가 비슷하다면 LSTM 모델이 LBP 이미지의 시계열 정보를 통해 제대로 된 분류를 하지 못한 것으로 분석된다. 그로 인해 BIG 2015의 결과와는 달리 CNN과 LSTM 앙상블 모델의 정확도가 떨어진 것이다. HOG 이미지 또한 생성되는 과정은 LBP와는 다르나 RAW 이미지가 갖고 있던 정보를 변형시킨 것이라는 점과 생성되는 이미지의 특성상 픽셀 하나하나 순서를 가지고 모델에 입력하는 LSTM으로는 유의미한 결과를 얻기가 힘들기 때문에 LSTM이 제대로 작동되지 않았다. 단일 모델에서 CNN과 LSTM 앙상블의 정확도가 상승되었다고 하나 정보가 변형된 이미지의 경우 현실의 데이터를 사용하였을 때 높은 정확도를 얻기 힘들 것이다.

5. 결 론

본 논문에서는 새로운 악성코드가 나타남에 따라 악성코드를 대처하는 데에 유용한 딥러닝을 이용해 악성코드를 분류할 때 분류의 정확도를 높이고 데이터 수집 후 각 클래스 간의 데이터 불균형이 생겼을 때 정확도를 높이는 방법을 제안하고 다양한 데이터를 분석하였다.

LBP와 HOG 알고리즘을 적용해 모델에 학습시켜 정확도를 분석하였다. 실험 결과, 악성코드 이미지에서 엣지 성분이 아닌 텍스쳐가 더 중요한 특성임을 확인하였고 이미지가 변형되지 않고 픽셀에 시계열 정보가 남아있을수록 일반적인 CNN 앙상블 모델보다 LSTM이 추가된 앙상블 모델이 정확도가 더 높다는 것을 확인하였다. 또한, 원본 이미지의 특성이 변형되더라도 CNN 단일모델보다 CNN 앙상블 모델이 전체적으로 높은 정확도를 보였다.

향후 연구에서는 새롭게 발견된 악성코드가 기존의 악성코드 패밀리로 정의되지 않을 수 있기 때문에 새로운 악성코드들을 분류하기 위해 정답 라벨 없이 비슷한 특징끼리 군집화를 하는 비지도 학습을 이용하여 악성코드의 이미지에서 특징을 추출하는 방법을 연구하고자 한다.

References

[1] “Cyber Threat Prospects for 2021”, KISA, Jan. 26, 2021 [Internet], https://krcert.or.kr/data/reportView.do?bulletin_writing_sequence=35878.

[2] C. Beek, et al., 2021 McAfee Threats report [Internet], https://www. mcafee.com/enterprise/en-us/lp/threats-reports/jun-2021.html.

[3] Press Release, WatchGuard, Jun. 24, 2021 [Internet], https://www. watchguard.com/wgrd-news/press-releases/new-watchguard-research-reveals-traditional-anti-malware-solutions-miss.

[4] L. Nataraj, S. Karthikeyan, G. Jacob, and B. S. Manjunath, “Malware images: Visualization and automatic classification,” *Proceedings of the 8th International Symposium on Visualization for Cyber Security*, No.4, pp.1-7, 2011.

[5] H. Kim and M. Kim, “Image-based malware classification system using image preprocessing and ensemble techniques,” *Proceedings of the Korea Information Processing Society Conference. Korea Information Processing Society*, pp.715-718, 2021.

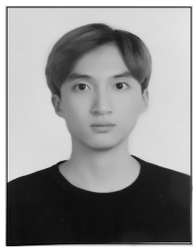
[6] M. Sahin and S. Bahtiyar, “A survey on malware detection with deep learning,” *13th International Conference on Security of Information and Networks*, No.34, pp.1-6, 2020.

[7] S. Kim, D. Kim, H. Lee, and T. Lee, “A study on classification of CNN-based linux malware using image processing techniques,” *Journal of the Korea Academia-Industrial cooperation Society*, Vol.21, No.9, pp.634-642, 2020.

[8] S. Yue, “Imbalanced malware images classification: A CNN based approach,” *arXiv preprint arXiv:1708.08042*, 2017.

[9] T. Ojala, M. Pietikäinen, and D. Harwood, “A comparative study of texture measures with classification based on featured distributions,” *Pattern Recognition*, Vol.29, No.1, pp.51-59, 1996.

[10] N. Dalal and B. Triggs, "Histograms of oriented gradients for human detection," *International Conference on Computer Vision & Pattern Recognition (CVPR)*, San Diego, UnitedStates, pp.886-893, 2005.
[11] K. O'Shea and R. Nash, "An introduction to convolutional neural networks," *arXiv preprint arXiv:1511.08458*, 2015.
[12] S. Hochreiter and J. Schmidhuber, "LONG SHORT-TERM MEMORY," *Neural Computation*, Vol.9, No.8, pp.1735-1780, 1997.
[13] R. O'Brien and H. Ishwaran, "A random forests quantile classifier for class imbalanced data," *Pattern Recognition*, Vol.90, pp.232-249, 2019.
[14] F. Provost, "Machine learning from imbalanced data sets 101," *Proceedings of the AAAI 2000 Workshop on Imbalanced Data Sets*, pp.1-3, 2000.
[15] R. Ronen, M. Radu, C. Feuerstein, E. Yom-Tov, and M. Ahmadi, "Microsoft malware classification challenge," *arXiv preprint arXiv:1802.10135*, 2018.



김 해 수
https://orcid.org/0000-0003-1844-1958
e-mail : ww232330@hknu.ac.kr
2022년 한경대학교 컴퓨터응용수학부 (학사)
현 재 한경대학교 컴퓨터응용수학부 석사과정
관심분야 : 네트워크 보안, 인공지능, 네트워크 슬라이싱, 자연어 처리

김 미 희
https://orcid.org/0000-0002-4896-7400
e-mail : mhkim@hknu.ac.kr
1997년 이화여자대학교 전자계산학과 (학사)
1999년 이화여자대학교 컴퓨터학과(석사)
1999년 ~ 2003년 한국전자통신연구원 연구원
2007년 이화여자대학교 컴퓨터학과(박사)
2007년 ~ 2009년 이화여자대학교 컴퓨터학과 전임강사
2009년 ~ 2010년 노스캐롤라이나주립대학교 연구원
2011년 ~ 현 재 한경대학교 컴퓨터응용수학부 컴퓨터시스템연구소 교수
관심분야 : 네트워크 성능 분석 및 보안, 무선네트워크 보안, 침입대응, 크라우드센싱, 블록체인