(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2024-0106617
(43) 공개일자 2024년07월08일

(51) 국제특허분류(Int. Cl.)
G06F 21/56 (2013.01) *G06F 16/35* (2019.01)
G06N 3/0464 (2023.01) *G06V 10/764* (2022.01)
(52) CPC특허분류
G06F 21/56 (2013.01)
G06F 16/35 (2019.01)
(21) 출원번호 10-2022-0189564
(22) 출원일자 2022년12월29일
심사청구일자 2022년12월29일

(71) 출원인
충남대학교산학협력단
대전광역시 유성구 대학로 99 (궁동, 충남대학교)
(72) 발명자
조은선
대전광역시 유성구 어은로 57, 110동 1504호(어은동, 한빛아파트)
백준영
대전광역시 중구 문화로 99번길 44-1
김정우
대전광역시 유성구 대학로76번안길 45, 101동 204호(궁동, 시티팰리스)
(74) 대리인
이은철, 김재문

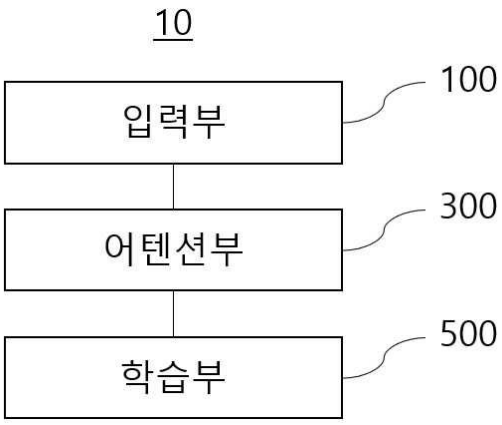
전체 청구항 수 : 총 6 항

(54) 발명의 명칭 **악성코드 패밀리 학습장치 및 이를 이용한 악성코드 패밀리 식별장치**

(57) 요 약

본 발명은, 악성코드 패밀리로 각각 라벨링된 악성코드 이미지와 구조 엔트로피를 입력받는 입력부; 상기 악성코드 이미지와 상기 구조 엔트로피에 대해 크로스모달 어텐션을 수행하여 정보를 상호보완하는 어텐션부; 상기 어텐션부를 통해 상호보완된 악성코드 이미지가 제1 CNN(Convolutional Neural Network) 모델에 입력되고 상기 어텐션부를 통해 상호보완된 구조 엔트로피가 제2 CNN 모델에 입력되어 특징(feature)이 추출되며, 추출된 특징이 완전연결 계층(Fully Connected Layer)에 입력되어 학습되는 학습부;를 포함하는 것을 일 특징으로 한다.

대 표 도 - 도1



(52) CPC특허분류
G06N 3/0464 (2023.01)

이 발명을 지원한 국가연구개발사업
과제고유번호 1711160654
과제번호 2022-0-01200-001
부처명 과학기술정보통신부
과제관리(전문)기관명 정보통신기획평가원
연구사업명 정보통신방송혁신인재양성
연구과제명 융합보안대학원(충남대학교)
기 여 율 1/1
과제수행기관명 충남대학교 산학협력단
연구기간 2022.01.01 ~ 2022.12.31

명 세 서

청구범위

청구항 1

악성코드 패밀리로 각각 라벨링된 악성코드 이미지와 구조 엔트로피를 입력받는 입력부;

상기 악성코드 이미지와 상기 구조 엔트로피에 대해 크로스모달 어텐션을 수행하여 정보를 상호보완하는 어텐션부;

상기 어텐션부를 통해 상호보완된 악성코드 이미지가 제1 CNN(Convolutional Neural Network) 모델에 입력되고 상기 어텐션부를 통해 상호보완된 구조 엔트로피가 제2 CNN 모델에 입력되어 특징(feature)이 추출되며, 추출된 특징이 완전연결 계층(Fully Connected Layer)에 입력되어 학습되는 학습부;를

포함하는 악성코드 패밀리를 분류하기 위한 학습장치.

청구항 2

제 1 항에 있어서,

상기 입력부는,

악성코드를 일정한 청크 단위로 쪼개고 각 청크의 바이트의 빈도를 기반으로 엔트로피를 계산하여 상기 구조 엔트로피를 입력받고, One-hot 인코딩을 통해 상기 구조 엔트로피에 위치정보를 추가하는 것을 특징으로 하는 악성코드 패밀리를 분류하기 위한 학습장치.

청구항 3

제 1 항에 있어서,

상기 입력부는,

악성코드의 1바이트를 0에서 255 사이의 픽셀값으로 변환하여 상기 악성코드 이미지를 입력받고, 입력된 이미지를 다운샘플링하는 것을 특징으로 하는 악성코드 패밀리를 분류하기 위한 학습장치.

청구항 4

제 1 항에 있어서,

상기 어텐션부는,

크로스모달 어텐션 수행을 위해 상기 악성코드 이미지와 상기 구조 엔트로피를 커널의 크기가 1인 1D convolutional layer를 통해 임베딩하는 것을 특징으로 하는 악성코드 패밀리를 분류하기 위한 학습장치.

청구항 5

악성코드 이미지와 구조 엔트로피를 입력받는 입력부;

상기 악성코드 이미지와 상기 구조 엔트로피에 대해 크로스모달 어텐션을 수행하여 정보를 상호보완하는 어텐션부;

악성코드 패밀리로 각각 라벨링된 악성코드 이미지와 구조 엔트로피로 학습된 심층 인공신경망을 이용하여, 상기 어텐션부를 통해 상호보완된 악성코드 이미지와 구조 엔트로피에 존재하는 악성코드의 패밀리를 분류하는 분

류부;를

포함하는 악성코드 패밀리를 분류하기 위한 식별장치.

청구항 6

제 5 항에 있어서,

상기 분류부는,

상호보완된 악성코드 이미지가 제1 CNN(Convolutional Neural Network) 모델에 입력되고 상호보완된 구조 엔트로피가 제2 CNN 모델에 입력되어 특징(feature)이 추출되며, 추출된 특징이 완전연결 계층(Fully Connected Layer)에 입력되어 학습된 심층 인공신경망을 이용하는 것을 특징으로 하는 악성코드 패밀리를 분류하기 위한 식별장치.

발명의 설명

기 술 분 야

[0001] 본 발명은 악성코드 패밀리 학습장치 및 이를 이용한 악성코드 패밀리 식별장치에 관한 것으로서, 특히 딥러닝 기반으로 악성코드의 패밀리를 분류하고 식별하기 위한 학습장치 및 식별장치에 관한 것이다.

배 경 기 술

[0003] 악성코드는 지난 수십 년 동안 사이버보안을 크게 위협하였고, 해를 거듭할수록 그 수가 증가하고 공격 기술 또한 정교해지고 있다. 따라서, 악성코드에 대처하는 것은 시급한 문제가 되었다. 악성코드에 대처하기 위해서는 악성코드의 일반적인 행위와 악성코드가 속하는 패밀리를 파악하는 것이 중요하다. 악성코드 패밀리를 파악하기 위해서는 디스어셈블을 통한 분석이 필수적인데, 이는 비용이 큰 작업이다. 난독화 기술의 발달은 악성코드의 디스어셈블을 어렵게 만들고 있다. 따라서 악성코드를 디스어셈블하지 않고 이미지로 변환하여 변환된 이미지를 기반으로 악성코드 패밀리를 분류하는 연구들이 제안되었다.

[0004] 다른 연구들은 악성코드에서 추출된 구조 엔트로피를 기반으로 악성코드 패밀리를 분류한다. 구조 엔트로피는 악성코드를 디스어셈블하지 않고 얻어낼 수 있으며 파일에 적용된 난독화에 덜 민감하다는 장점이 있다. 그러나 악성코드 이미지와 구조 엔트로피는 서로 다른 측면에서 각자의 단점을 가진다.

[0005] 딥러닝은 학습데이터의 특징을 스스로 학습한다는 장점이 있어 데이터에 대한 가공이 적으며, 이 때문에 악성코드 탐지 및 분류를 위해 활용되고 있다. 악성코드를 분류하는 방법으로 악성코드를 그레이 스케일 이미지로 변환하여 CNN을 기반으로 악성코드 패밀리를 분류하는 방법이 있다. 이외에도 N-gram, Raw Byte의 데이터가 악성코드 분석에 활용된다. 또한, 다양한 종류의 데이터를 효과적으로 결합하는 멀티모달 러닝 역시 악성코드 탐지 및 분류를 위해 사용된다.

[0006] 따라서, 이미지 변환을 이용한 방법과 구조 엔트로피를 이용하는 방법의 장점을 모두 아우를 수 있는 바이너리 이미지와 구조 엔트로피를 사용하는 악성코드 패밀리 학습장치 및 식별장치가 요구되고 있는 실정이다.

발명의 내용

해결하려는 과제

[0008] 본 발명은 이미지와 엔트로피 정보를 모두 이용하여 악성코드 패밀리를 분류하는 악성코드 패밀리를 분류하기 위한 학습장치 및 이를 이용한 악성코드 패밀리 식별장치를 제공하는 것을 목적으로 한다.

과제의 해결 수단

[0010] 상기 목적을 달성하기 위하여 본 발명은, 악성코드 패밀리로 각각 라벨링된 악성코드 이미지와 구조 엔트로피를 입력받는 입력부; 상기 악성코드 이미지와 상기 구조 엔트로피에 대해 크로스모달 어텐션을 수행하여 정보를 상호보완하는 어텐션부; 상기 어텐션부를 통해 상호보완된 악성코드 이미지가 제1 CNN(Convolutional Neural Network) 모델에 입력되고 상기 어텐션부를 통해 상호보완된 구조 엔트로피가 제2 CNN 모델에 입력되어 특징(feature)이 추출되며, 추출된 특징이 완전연결 계층(Fully Connected Layer)에 입력되어 학습되는 학습부;를 포함하는 것을 일 특징으로 한다.

[0011] 바람직하게는, 상기 입력부는, 악성코드를 일정한 청크 단위로 쪼개고 각 청크의 바이트의 빈도를 기반으로 엔트로피를 계산하여 상기 구조 엔트로피를 입력받고, One-hot 인코딩을 통해 상기 구조 엔트로피에 위치정보를 추가할 수 있다.

[0012] 바람직하게는, 상기 입력부는, 악성코드의 1바이트를 0에서 255 사이의 픽셀값으로 변환하여 상기 악성코드 이미지를 입력받고, 입력된 이미지를 다운샘플링할 수 있다.

[0013] 바람직하게는, 상기 어텐션부는, 크로스모달 어텐션 수행을 위해 상기 악성코드 이미지와 상기 구조 엔트로피를 커널의 크기가 1인 1D convolutional layer를 통해 임베딩할 수 있다.

[0014] 또한 본 발명은, 악성코드 이미지와 구조 엔트로피를 입력받는 입력부; 상기 악성코드 이미지와 상기 구조 엔트로피에 대해 크로스모달 어텐션을 수행하여 정보를 상호보완하는 어텐션부; 악성코드 패밀리로 각각 라벨링된 악성코드 이미지와 구조 엔트로피로 학습된 심층 인공신경망을 이용하여, 상기 어텐션부를 통해 상호보완된 악성코드 이미지와 구조 엔트로피에 존재하는 악성코드의 패밀리를 분류하는 분류부;를 포함하는 것을 다른 특징으로 한다.

[0015] 바람직하게는, 상기 분류부는, 상호보완된 악성코드 이미지가 제1 CNN(Convolutional Neural Network) 모델에 입력되고 상호보완된 구조 엔트로피가 제2 CNN 모델에 입력되어 특징(feature)이 추출되며, 추출된 특징이 완전연결 계층(Fully Connected Layer)에 입력되어 학습된 심층 인공신경망을 이용할 수 있다.

발명의 효과

[0017] 본 발명은 바이너리 코드의 행위를 분석하는 과정에서 악성코드 패밀리를 조기에 파악하여 정확한 악성 행위를 도출할 수 있다는 이점이 있다.

[0018] 또한, 본 발명은 악성코드 패밀리 식별을 통해 악성코드에 대한 대응방안 수립에 도움을 줄 수 있다는 이점이 있다.

도면의 간단한 설명

[0020] 도 1은 본 발명의 실시예에 따른 악성코드 패밀리를 분류하기 위한 학습장치의 구성도를 나타낸다.

도 2은 본 발명의 실시예에 따른 어텐션부의 크로스모달 어텐션 모델을 나타낸다.

도 3는 본 발명의 실시예에 따른 어텐션부의 크로스모달 어텐션 과정을 나타낸다.

도 4는 본 발명의 실시예에 따른 악성코드 패밀리를 분류하기 위한 학습장치의 딥러닝 모델 구조를 나타낸다.

도 5는 본 발명의 실시예에 따른 악성코드 패밀리를 분류하기 위한 식별장치의 구성도를 나타낸다.

도 6은 본 발명의 실시예에 따른 9개의 패밀리 악성코드의 데이터셋을 나타낸다.

도 7은 본 발명의 실시예에 다른 악성코드 패밀리 분류 성능 비교표를 나타낸다.

발명을 실시하기 위한 구체적인 내용

[0021] 이하, 첨부된 도면들에 기재된 내용들을 참조하여 본 발명을 상세히 설명한다. 다만, 본 발명이 예시적 실시 예들에 의해 제한되거나 한정되는 것은 아니다. 각 도면에 제시된 동일 참조부호는 실질적으로 동일한 기능을 수행하는 부재를 나타낸다.

[0022] 본 발명의 목적 및 효과는 하기의 설명에 의해서 자연스럽게 이해되거나 보다 분명해 질 수 있으며, 하기의 기

재만으로 본 발명의 목적 및 효과가 제한되는 것은 아니다. 또한, 본 발명을 설명함에 있어서 본 발명과 관련된 공지 기술에 대한 구체적인 설명이, 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명을 생략하기로 한다.

[0023] 도 1은 본 발명의 실시예에 따른 악성코드 패밀리를 분류하기 위한 학습장치(10)의 구성도를 나타낸다. 도 1을 참조하면, 악성코드 패밀리를 분류하기 위한 학습장치(10)는 입력부(100), 어텐션부(300), 및 학습부(500)를 포함할 수 있다.

[0024] 악성코드 패밀리를 분류하기 위한 학습장치(10)는 구조 엔트로피와 악성코드 이미지의 단점을 상호보완하는 어텐션 기반의 크로스모달 CNN을 구조를 채택하였다. 악성코드 패밀리를 분류하기 위한 학습장치(10)는 악성코드 패밀리 분류를 위한 학습이며, 입력 데이터는 악성코드 이미지와 구조 엔트로피이다. 악성코드 패밀리를 분류하기 위한 학습장치(10)는 서로 다른 두 개의 데이터를 어텐션 메커니즘을 통해 효과적으로 결합하고 기존의 하나의 데이터만을 사용해서 악성코드 패밀리를 분류할 때보다 더 높은 정확도를 보인다.

[0025] 입력부(100)는 악성코드 패밀리로 각각 라벨링된 악성코드 이미지와 구조 엔트로피를 입력받을 수 있다.

[0026] 입력부(100)는 악성코드를 일정한 청크 단위로 쪼개고 각 청크의 바이트의 빈도를 기반으로 엔트로피를 계산하여 구조 엔트로피를 입력받고, One-hot 인코딩을 통해 상기 구조 엔트로피에 위치정보를 추가할 수 있다. 엔트로피 계산식은 아래의 [수학식 1]과 같다.

[0027] [수학식 1]

[0028] $$H(x) = -\sum_{j=1}^{n} p(x_j)\log_2 p(x_j)$$

[0029] 입력부(100)는 One-hot 인코딩을 통해 파일의 바이트 정보만을 고려하여 일반적인 악성코드에서 중요하게 다루어지는 위치정보를 효과적으로 처리하지 못한다는 문제점을 해결할 수 있다.

[0030] 입력부(100)는 악성코드의 1바이트를 0에서 255 사이의 픽셀값으로 변환하여 상기 악성코드 이미지를 입력받고, 입력된 이미지를 다운샘플링할 수 있다. 입력된 이미지는 64*784로 다운샘플링 될 수 있다.

[0031] 어텐션부(300)는 악성코드 이미지와 구조 엔트로피에 대해 크로스모달 어텐션을 수행하여 정보를 상호보완할 수 있다.

[0032] 악성코드 이미지는 악성코드의 전체적인 정보를 효과적으로 표현할 수 있지만, 이미지에 노이즈가 생길 수 있는 난독화 또는 암호화 등의 기술에 영향을 많이 받는다는 단점이 있다. 파일의 위치정보를 반영한 구조 엔트로피는 바이트의 빈도를 기반으로 엔트로피 계산되며 난독화에 강인하다는 장점이 있으나 엔트로피를 추출하는 과정에서 악성코드에 대한 일부 정보를 손실할 수 있다는 단점이있다.

[0033] 어텐션부(300)는 크로스모달 어텐션을 기반으로 두 개의 데이터를 효과적으로 결합하고 이미지와 구조 엔트로피가 서로의 정보를 참조하여 단점을 보완하며 학습하게 할 수 있다.

[0034] 어텐션부(300)는 다른 데이터에 대해 정보를 얻기 위한 어텐션 벡터 W_a 를 score함수를 기반으로 학습하는 어텐션 메커니즘([수학식 2])을 이용할 수 있다. 어텐션 메커니즘에서 데이터 S는 학습된 W_a 를 통해 score함수의 값에 기반하여 데이터 h이 정보를 효과적으로 참조할 수 있다.

[0035] [수학식 2]

[0036] $$score(S,h)=S^{T}*W_a*h$$

[0037] 어텐션부(300)는 학습부(500)가 서로 다른 데이터를 두 개 이상의 모달리티에 기반하여 학습하는 멀티 모달 러닝이 가능하도록 크로스모달 어텐션을 수행할 수 있다. 멀티 모달 러닝을 통해 다른 유형을 데이터를 융합하여 학습할 수 있다.

[0038] 도 2는 본 발명의 실시예에 따른 어텐션부(300)의 크로스모달 어텐션 모델을 나타내고, 도 3은 본 발명의 실시예에 따른 어텐션부의 크로스모달 어텐션 과정을 나타낸다. 도 2와 도 3을 참조하면, 어텐션부(300)는 이미지와 구조 엔트로피의 단점을 서로 보완하며 학습시키기 위해 크로스모달 어텐션을 사용할 수 있다. 어텐션부(300)는 크로스모달 어텐션 수행을 위해 악성코드 이미지와 구조 엔트로피를 커널의 크기가 1인 1D convolutional layer

를 통해 임베딩([수학식 3])할 수 있다.

[0039] [수학식 3]

[0040] $$X = Conv1D(X,k_1) \in \mathbb{R}^d$$

[0041] 어텐션부(300)는 임베딩된 각 데이터를 어텐션 연산을 통해 서로의 정보를 참조하게 할 수 있다. 데이터 X가 데이터 Y를 타겟으로 하는 어텐션 연산은 [수학식 4]와 같다. 어텐션 연산을 통해 X는 Y에 대한 정보를 W_a를 통해 참조한다. 위와 같은 어텐션 연산을 Y에서 X 양방향으로도 계산하여 크로스모달 어텐션을 계산한다. 계산을 통해 두 학습데이터는 서로의 정보를 효과적으로 참조한다.

[0042] [수학식 4]

$$score(X,Y) = X^T * W_a * Y$$
$$A = softmax(score(X,Y))$$
$$A_Y = \sum_{i=1} Y_i * A_i$$
$$X = [X, A_Y]$$

[0043]

[0044] 도 4는 본 발명의 실시예에 따른 악성코드 패밀리를 분류하기 위한 학습장치(10)의 딥러닝 모델 구조를 나타낸다. 도 4를 참조하면, 학습부(500)는 어텐션부(300)를 통해 상호보완된 악성코드 이미지가 제1 CNN(Convolutional Neural Network) 모델에 입력되고 어텐션부(300)를 통해 상호보완된 구조 엔트로피가 제2 CNN 모델에 입력되어 특징(feature)이 추출되며, 추출된 특징이 완전연결 계층(Fully Connected Layer)에 입력되어 학습될 수 있다.

[0045] 학습부(500)는 악성코드 패밀리 분류를 위해 패턴인식에 강력한 CNN을 기반으로 모델이 구성될 수 있다. CNN은 강력한 패턴인식이 가능한 뉴럴 네트워크로 저수준의 데이터에서 고수준의 특징을 효과적으로 추출할 수 있다. CNN은 1D convolutional layer 4개를 쌓아 구성되며, 각각의 레이어는 max-pooling, normalization layer를 거칠 수 있다.

[0046] 도 5는 본 발명의 실시예에 따른 악성코드 패밀리를 분류하기 위한 식별장치(30)의 구성도를 나타낸다. 도 5를 참조하면, 악성코드 패밀리를 분류하기 위한 식별장치(30)는 입력부(100), 어텐션부(300), 및 분류부(500)를 포함할 수 있다.

[0047] 입력부(100)는 악성코드 이미지와 구조 엔트로피를 입력받을 수 있다. 입력부(100)는 전술한 악성코드 패밀리를 분류하기 위한 학습장치(10)에서 사용되는 것과 동일한 기능과 구조를 갖는다.

[0048] 어텐션부(300)는 악성코드 이미지와 구조 엔트로피에 대해 크로스모달 어텐션을 수행하여 정보를 상호보완할 수 있다. 어텐션부(300)는 전술한 악성코드 패밀리를 분류하기 위한 학습장치(10)에서 사용되는 것과 동일한 기능과 구조를 갖는다.

[0049] 분류부(500)는 악성코드 패밀리로 각각 라벨링된 악성코드 이미지와 구조 엔트로피로 학습된 심층 인공신경망을 이용하여, 어텐션부(300)를 통해 상호보완된 악성코드 이미지와 구조 엔트로피에 존재하는 악성코드의 패밀리를 분류할 수 있다.

[0050] 분류부(500)는 상호보완된 악성코드 이미지가 제1 CNN(Convolutional Neural Network) 모델에 입력되고 상호보완된 구조 엔트로피가 제2 CNN 모델에 입력되어 특징(feature)이 추출되며, 추출된 특징이 완전연결 계층(Fully Connected Layer)에 입력되어 학습된 심층 인공신경망을 이용할 수 있다. 분류부(500)에서 사용되는 인공신경망은 전술한 악성코드 패밀리를 분류하기 위한 학습장치(10)에서 학습될 수 있다.

[0051] **이하에서는 악성코드 패밀리를 분류하기 위한 식별장치(30)의 성능 평가 결과를 살펴본다.**

[0052] 악성코드 패밀리를 분류하기 위한 식별장치(30)의 성능을 평가하기 위해 이 미지로 학습된 CNN기반의 악성코드 분류기와 구조 엔트로피로 학습된 CNN기반의 악성코드 분류기를 재현하여 성능을 비교하였다. 성능 지표는 정확도 그리고 정밀도와 재현율의 가중 평균인 F1-score이다.

[0053] 도 6은 본 발명의 실시예에 따른 9개의 패밀리 악성코드의 데이터셋을 나타낸다. 도 6을 참조하면, 악성코드 패밀리를 분류하기 위한 식별장치(30)를 학습, 평가하기 위해 Kaggle의 Microsoft Malware Classification Challenge(BIG-2015)를 사용한다. BIG-2015는 9개의 패밀리의 악성코드 10868개를 포함하며 데이터셋의 세부내

용은 도 6과 같다. 적은 샘플 수의 클래스의 악성코드에 대한 정확도를 확인하기 위해 10-fold-validation을 적용해서 모델의 성능을 평가하였다.

[0054] 도 7은 본 발명의 실시예에 다른 악성코드 패밀리 분류 성능 비교표를 나타낸다. 도 7을 참조하면, 크로스 모달 CNN(Model 6)과 재현된 다른 분류기와의 성능 비교 표이다. Model 1, 2는 성능 비교를 위해 구현된 이미지와 구조 엔트로피로 학습된 CNN 모델이다. 모델 3, 4는 타 논문에서 제안한 이미지와 구조 엔트로피로 학습된 CNN 모델이며, 모델 5는 제안하는 모델에서 크로스모달 어텐션이 제거된 Late Fusion방식의 멀티 모달 CNN 모델이다. 도 7의 결과를 확인했을 때 제안하는 모델은 높은 성능으로 악성코드 패밀리를 분류했으며 이미지 또는 구조 엔트로피 하나의 데이터로만 학습된 분류기보다 정확도는 0.41, F1-score는 0.272의 성능 향상을 보였다. 또한, 엔트로피와 악성코드 이미지를 사용한 기존 연구보다도 높은 성능을 보여주었다.

[0055] 제안하는 어텐션 기반의 크로스모달 CNN은 크로스모달 어텐션이 적용되지 않은 모델 5와 비교했을 때도 더 높은 성능으로 악성코드를 분류한다. 이를 통해 본 연구에서 제안하는 크로스모달 어텐션이 악성코드 이미지와 구조 엔트로피를 결합하는 효과적인 방법임을 반증한다.

[0056] 이상에서 대표적인 실시예를 통하여 본 발명을 상세하게 설명하였으나, 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자는 상술한 실시예에 대하여 본 발명의 범주에서 벗어나지 않는 한도 내에서 다양한 변형이 가능함을 이해할 것이다. 그러므로 본 발명의 권리 범위는 설명한 실시예에 국한되어 정해져서는 안 되며, 후술하는 특허청구범위뿐만 아니라 특허청구범위와 균등 개념으로부터 도출되는 모든 변경 또는 변형된 형태에 의하여 정해져야 한다.

부호의 설명

[0058] 10 : 악성코드 패밀리를 분류하기 위한 학습장치

30 : 악성코드 패밀리를 분류하기 위한 식별장치

100 : 입력부

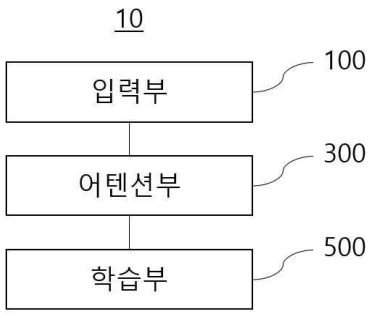
300 : 어텐션부

500 : 학습부

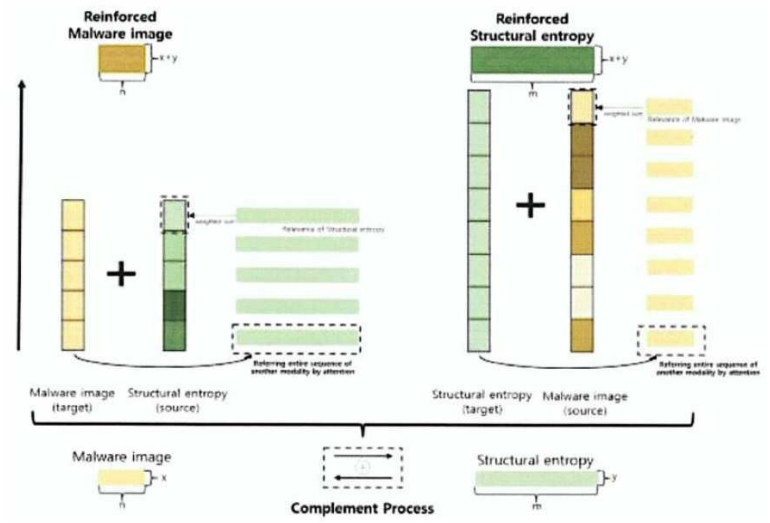
700 : 분류부

도면

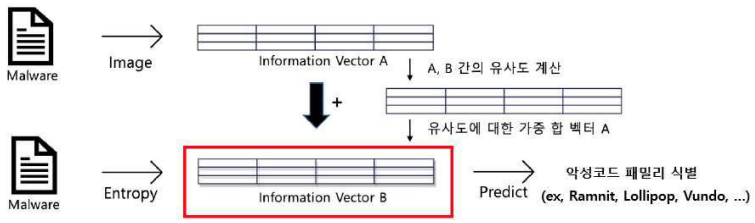
도면1



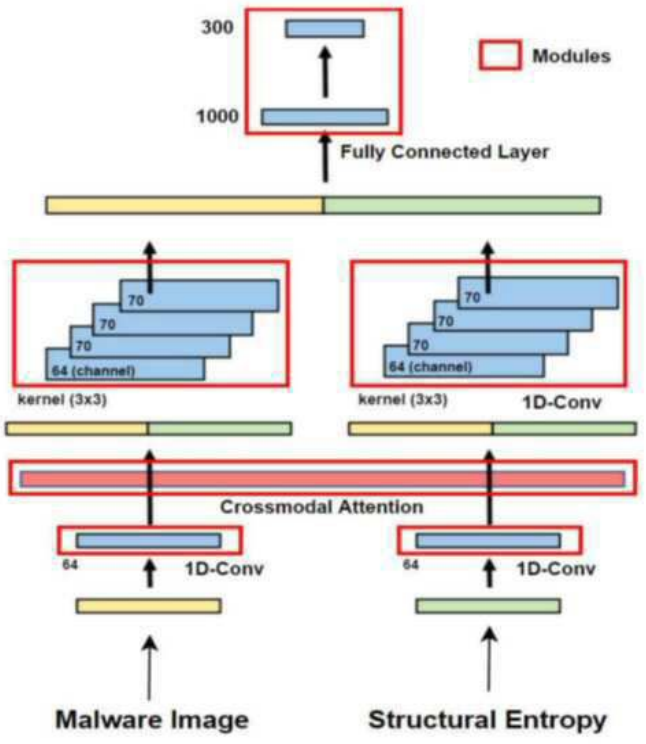
도면2


Reinforced
Malware image
Reinforced
Structural entropy
Malware image
(target)
Structural entropy
(source)
Structural entropy
(target)
Malware image
(source)
Malware image
Structural entropy
Complement Process

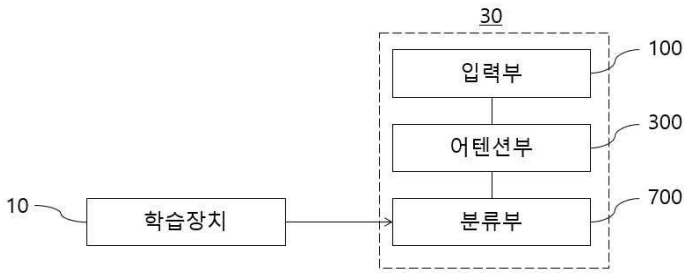
도면3


Malware
Image
Information Vector A
A, B 간의 유사도 계산
유사도에 대한 가중 합 벡터 A
Malware
Entropy
Information Vector B
Predict
악성코드 패밀리 식별
(ex, Ramnit, Lollipop, Vundo, ...)

도면4


300
1000
Modules
Fully Connected Layer
70
70
70
64 (channel)
kernel (3x3)
70
70
70
64 (channel)
kernel (3x3)
1D-Conv
Crossmodal Attention
64
1D-Conv
64
1D-Conv
Malware Image
Structural Entropy

도면5



도면6

Family	ClassID	#samples
Ramnit	1	1541
Lollipop	2	2478
Kelihos_ver3	3	2942
Vundo	4	475
Simda	5	42
Tracur	6	751
Kelihos_ver1	7	398
Obfuscator.ACY	8	1228
Gatak	9	1013

도면7

Model	Data	Acc	F1-score
1	Entropy (w/ location info)	97.95	0.9362
2	Image	96.21	0.9010
3	Entropy[4] (w/o location info)	97.03	0.9305
4	Image[1]	97.5	0.9400
5	Entropy, Image (w/ location info)	97.89	0.9301
6	Entropy, Image (w/ location info)	**98.36**	**0.9634**