L-022

画像特徴量によるマルウェア亜種検知に関する検討
A Study on Detection of variant of Malware by Image features

小寺 建輝† 泉 隆†
Tateki Kodera Takashi Izumi

1. はじめに

近年，マルウェア亜種自動生成ツールの流通や，マルウェアのソースコード流出により，亜種生成が簡易化・高速化され，ウイルス定義ファイル等のパターンファイルの作成・配布が追い付かない現状となっている.例えば，IoT マルウェアの 1 種である「Mirai」は作成者によってソースコードが公開されており，それを改変した亜種が大量に作成され，多くの IoT デバイスが感染の被害にあった．このような亜種検知に関する問題を解決するため，機械学習により亜種を検知・分類する研究が現在取り組まれている．その中でも，Windows 系マルウェアを画像化し，画像認識によって亜種を該当するファミリに分類する先行研究[1]では，高い識別精度でマルウェアを分類できたことが報告されている．これは，亜種が元のコードの一部のみを改変して作成されるため，元のマルウェアとその亜種，つまり同一ファミリでは視覚的に類似した画像が得られるためである．しかし，先行研究では，各ファミリの亜種と正常ファイルを識別することが検討されていない．

これらを踏まえて本研究では，同一ファミリ等の類似したマルウェアの画像同士をグループ化してグループごとに亜種の検知モデルを構築し，各検知モデルで亜種と正常ファイルを識別して亜種を検知する手法を検討する．

本稿では，グループごとの亜種検知モデルの構築及び亜種検知・識別時に利用する画像特徴量において，LBP(Local Binary Pattern)特徴量[2]を用いた場合と Gist 特徴量[3]を用いた場合の亜種検知率・誤検知率の比較を行い，亜種検知に有効な特徴量について検討をする．

2. マルウェア画像化

ファイルを画像化する手法[1]を以下に示す.また実際にマルウェアを画像化した例を図 1 に示す.

(1) 対象ファイルを 1Byte(8bit)ずつ読み込み 1 次元配列に格納する
(2) ファイルサイズ(配列の要素数)に応じて幅を決定し，2 次元配列に変換する
(3) 配列の要素の値は 1Byte であり，0-255 の範囲であるため，その値を画素値として 256 階調のグレースケール画像を生成する

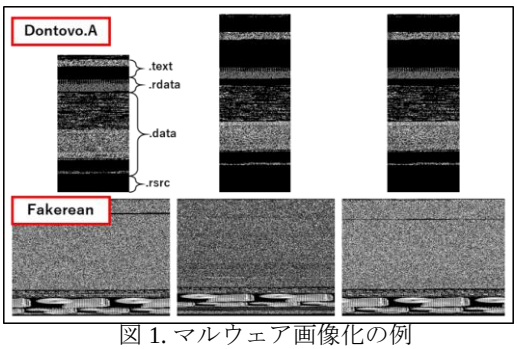

図 1. マルウェア画像化の例

† 日本大学 Nihon University

図 1 より，マルウェアを画像化すると PE ファイルのセクション(.text や.rdata 等)ごとに異なるテクスチャパターンがあらわれることが確認できる.また，1 章で述べたように，亜種が元のコードの一部のみを改変して作成されることから，同一ファミリで類似した画像が生成されていることも確認できる.

3. マルウェア亜種検知アルゴリズム

亜種検知モデルの学習及びそのモデルを利用して各ファミリの亜種と正常ファイルを識別するアルゴリズムを以下の 4 つのフェーズに分けて説明する.

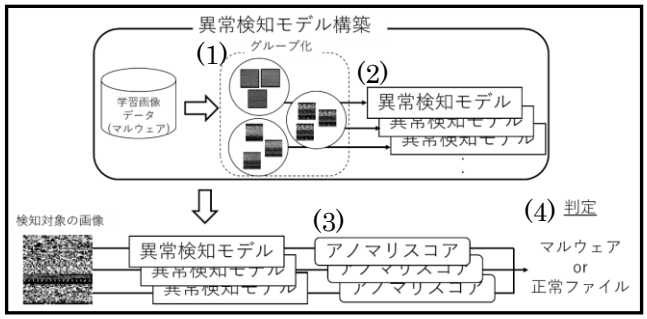

図 2. マルウェア亜種検知アルゴリズム概要

(1) 類似した画像のグループ化
学習データであるマルウェアにファミリ名のラベルを割り当て，ファミリごとにグループ化を行う．
本稿では検討しないが，他にも，クラスタリングを用いることにより，画像特徴量が類似したもの同士をグループ化する手法が考えられる．

(2) 異常検知モデルの構築
検知対象の画像が(1)で作成したグループに属するか否かをアノマリスコアにより判定する，異常検知モデルを各グループで構築する．また，判定のために各モデルでアノマリスコアに閾値を設定する．

(3) アノマリスコアの算出
検知対象の画像の特徴量を各異常検知モデルに入力し，アノマリスコアを算出する．

(4) マルウェアの判定
検知対象の画像のアノマリスコアがあるモデルで閾値未満であった場合，そのモデル(ファミリ)に該当するマルウェア(亜種)であると判定する．また，アノマリスコアが閾値以上であった場合，そのモデル(ファミリ)に非該当のファイルと判定する．
全てのモデル(ファミリ)において非該当のファイルと判定された画像を正常ファイルと識別する．

4. 実験

本実験で扱うマルウェアの画像は，図 1 に示したようにテクスチャ画像に類似していることから，各ファミリの異常検知モデルの構築及び異常検知モデルによる亜種検知を

行う際の画像特徴量として，テクスチャ画像の認識に利用される LBP 特徴量と Gist 特徴量を採用する.そして，各特徴量を用いた場合の亜種検知率（あるファミリのマルウェアを当該ファミリの亜種として正しく判定した割合）・誤検知率（正常ファイルをあるファミリの亜種として誤って判定した割合）の比較を各ファミリのモデルごとに行った.

ここで，モデルの構築及び亜種検知率の評価には Malimg Dataset[4]内の 25 ファミリ 9339 検体のマルウェアの画像と，誤検知率の評価に 913 検体の正常ファイルを利用して 10 分割交差検証を行う.表 1 に Malimg Dataset の内訳を示す.

また，モデル構築の学習アルゴリズム及びアノマリスコアの算出に Isolation Forest[5]を採用した.各モデルにおけるアノマリスコアの閾値は，線形判別分析法により決定した.

実験結果を図 3 に，Agent.FY ファミリのモデルにおいてアノマリスコアを算出した結果を図 4 に示す.

表 1. Malimg Dataset[4]の内訳

ファミリ名	タイプ	検体数
Adialer.C	Dialer	122
Agent.FYI	Backdoor	116
Allaple.A	Worm	2949
Allaple.L	Worm	1591
Alueron.gen!J	Trojan	198
Autorun.K	Worm:AutoIT	106
C2LOP.gen!g	Trojan	200
C2LOP.P	Trojan	146
Dialplatform.B	Dialer	177
Dontovo.A	Trojan Downloader	162
Fakerean	Rogue	381
Instantaccess	Dialer	431
Lolyda.AA1	PWS	213
Lolyda.AA2	PWS	184
Lolyda.AA3	PWS	123
Lolyda.AT	PWS	159
Malex.gen!J	Trojan	136
Obfuscator.AD	Trojan Downloader	142
Rbot!gen	Backdoor	158
Skintrim.N	Trojan	80
Swizzor.gen!E	Trojan Downloader	128
Swizzor.gen!I	Trojan Downloader	132
VB.AT	Worm	408
Wintrim.BX	Trojan Downloader	97
Yuner.A	Worm	800

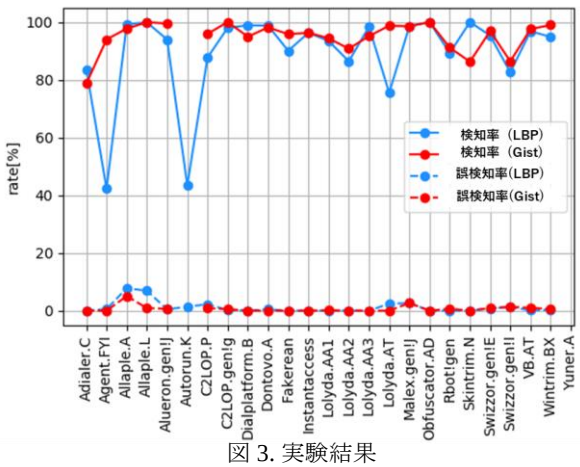

図 3. 実験結果

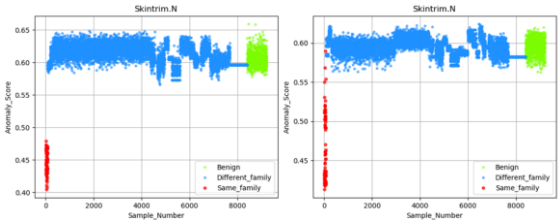

図 4. Agent.FYI のモデルにおけるアノマリスコア
（左:LBP 特徴量利用時，右:Gist 特徴量利用時）
赤:同一ファミリのマルウェア(亜種)，青:異なるファミリのマルウェア，緑:正常ファイル

図 3 より，亜種検知率が 100%となったのは LBP 特徴量・Gist 特徴量ともに 2 ファミリ，誤検知率が 0%となったのは LBP 特徴量で 10 ファミリ，Gist 特徴量で 11 ファミリとなった.そのうち，LBP 特徴量・Gist 特徴量ともに亜種検知率 100%かつ誤検知率 0%となったのは Obufuscator.AD の 1 ファミリであった.また，LBP 特徴量では平均亜種検知率が 89.3%，平均誤検知率が 1.2%であるのに対し，Gist 特徴量では平均亜種検知率が 95%，平均誤検知率が 0.7%であり，Gist 特徴量を用いた場合の方が安定した結果が得られた.しかし，図 3 中の Skintrim.N ファミリのように LBP 特徴量を用いた場合の方が，亜種検知率が高くなるファミリも少数確認された.これは図 4 より Skintrim.N ファミリでは，Gist 特徴量よりも，LBP 特徴量を用いた場合の方が同一ファミリのマルウェア（亜種）と正常ファイルのアノマリスコアの差が明確になったためである.このように，Gist 特徴量を用いた方が良い結果となるファミリや，LBP 特徴量を用いた方が良い結果となるファミリが確認され，ファミリごとに識別に有効な画像特徴量に違いがあらわれた.これを踏まえて，ファミリごとに利用する画像特徴量を分けることや複数の画像特徴量を組み合わせたモデルの構築を検討することで全体の検知精度が安定すると考えられる.

なお，図 3 において，LBP 特徴量・Gist 特徴量の Yuner.A, Gist 特徴量の Autorun.K の結果を欠損値としている．これは，ファミリ内の全検体の類似性が非常に高く特徴量が同一になってしまったため，Isolation Forest による異常検知モデルの構築に失敗したためである.

5. まとめ

本稿では，各グループでの検知モデルの構築及び亜種検知時に利用する画像特徴量において，LBP 特徴量を用いた場合と Gist 特徴量を用いた場合の亜種検知率・誤検知率の比較を行った.その結果，ファミリごとに識別に有効な画像特徴量に違いが現れることを確認した.

今後は，複数の画像特徴量を組み合わせや HLAC 特徴量等の別の画像特徴量を採用した際の亜種検知率・誤検知率を検証する.

参考文献

[1] L. Nataraj, et al. : ”Malware Images:Visualization and Automatic Classification”, VizSec’11(2011-07)
[2] DC.He and L.Wang : “Texture Unit, Texture Spectrum, And Texture Analysis”, Geoscience and Remote Sensing, IEEE Transactions on, Vol.28, pp.509-512(1990)
[3] A. Olivia and A. Torralba : ” Modeling the shape of a scene: a holistic representation of the spatial envelope”, Intl. Journal of Computer Vision, Vol.42, No.3, pp.145–175(2001)
[4] Abien Fred Agarap : “Malimg Dataset”, https://www.kaggle.com/afagarap/malimg-dataset (2018-06)
[5] Fei Tony Liu, et al. : “Isolation-Based Anomaly Detection”, ACM Transactions on Knowledge Discovery from Data(TKDD), Vol.6, No.1, pp.1-39(2013-03)