Revisão Sistemática da Literatura das Técnicas baseadas em Texturas para Classificação de *Malware*

Tamy E. Beppler[1], **Luiz E. S. Oliveira**[1], **André R. A. Grégio**[1]

[1]Departamento de Informática – Universidade Federal do Paraná (UFPR)
Caixa Postal 19097 – 81531-980 – Curitiba – PR – Brazil

{tebeppler, lesoliveira, gregio}@inf.ufpr.br

Abstract. *Malware attacks identification can be reduced to a problem of assigning a file under suspicion to a known malware family. Malware categorization into families requires the use of analysis and classification techniques. Recent research work show that texture analysis has been successfully applied technique for malware classification, because it is a fast, OS-agnostic approach, and achieves comparable results (in some cases more accurate) to traditional classification methods. In this paper, we present a study of different classification techniques based on texture analysis for malware assignment into families, as well as a discussion of their results.*

Resumo. *A identificação de ataques por malware pode ser resumida a um problema de atribuição do arquivo suspeito a uma família conhecida. A categorização de malware em famílias requer o uso de técnicas de análise e classificação. Pesquisas recentes mostram a análise de texturas como uma solução viável para tal fim, uma vez que se trata de uma abordagem rápida e independente de sistema operacional, além de alcançar resultados comparáveis (em alguns casos mais precisos) aos métodos de classificação tradicionais. Neste artigo, apresenta-se um levantamento de diferentes técnicas de classificação de malware em famílias usando texturas, bem como discute-se os resultados alcançados pela aplicação dessas técnicas.*

1. Introdução

Malware é uma ameaça à segurança de computadores e redes já há décadas. Programas maliciosos costumam ser classificados de acordo com seu objetivo de infecção e, conhecendo-o, é possível tomar contra-medidas [Nataraj 2015]. Devido ao grande volume de novas variantes de *malware* lançadas (segundo [Symantec 2017], mais de 357 milhões só em 2016), fica inviável fazer uma análise manual de cada exemplar. Buscando automatizar essa tarefa, foram desenvolvidas diversas maneiras de se realizar a análise dos arquivos, usualmente através da análise estática e da dinâmica. A estática busca identificar as características do arquivo sem executá-lo e a análise dinâmica observa o seu comportamento ao executá-lo [Damodaran et al. 2017].

A partir dos resultados da análise, pode-se diferenciar *malware* de arquivos benignos (detecção) [Idika and Mathur 2007] ou atribui-lo a uma dada família (classificação)

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001

[Nataraj 2015]. Em busca de uma classificação mais correta, diferentes abordagens foram propostas, como a análise por texturas, onde os arquivos binários são convertidos em imagens em escala de cinzas e utiliza-se um descritor para extrair as características da amostra [Nataraj et al. 2011a].

Neste artigo, é realizada uma revisão sistemática da literatura relacionada a classificação de *malware* baseada em análise de texturas, discutindo-se os bons resultados e as limitações de cada uma delas. O restante do artigo está dividido da seguinte forma: a Seção 2 apresenta conceitos básicos e discute os trabalhos relacionados; a Seção 3 exibe a metodologia utilizada para selecionar as pesquisas analisadas neste artigo; as técnicas de classificação de *malware* baseada em análise de textura encontradas na literatura são mostradas na Seção 4; a comparação e categorização das pesquisas a partir de suas características em comum é feita na Seção 5; por fim, as conclusões e trabalhos futuros estão na Seção 6.

2. Conceitos Básicos e Trabalhos Relacionados

Na análise por texturas, é necessário converter o binário do arquivo em uma imagem em escala de cinzas. Cada *byte* do arquivo é representado por sua cor correspondente (0, preto; 255, branco) e é previamente fixada uma largura (256 *bytes*). Para um processamento ainda mais rápido, alguns autores realizam um redimensionamento da imagem, tornando-a quadrada e utilizam um descritor de textura para extrair as características a serem utilizadas como entrada de um classificador, supervisionado ou não [Sathya and Abraham 2013] [Singh 2017].

Descritores de textura podem ser globais ou locais, ou seja, que analisam a imagem de maneira global ou por regiões [Bannour et al. 2009]. Os artigos que foram analisados nessa pesquisa utilizam descritores de ambos, como GIST [Oliva and Torralba 2001], *Color Layout Descriptor* (CLD) e *Homogenous Texture Descriptor* (HTD) [Manjunath et al. 2001], *Gabor Wavelet Transform* (GWT) [Manjunath and Ma 1996], *Discrete Wavelet Transform* (DWT) [Shensa 1992], *Local Binary Pattern* (LBP) [Ojala et al. 2002].

Diversos classificadores podem ser utilizados para esse fim, como por exemplo *Stochastic Gradient Descent* (SGD) [Robbins and Monro 1985], *Support Vector Machine* (SVM) [Cortes and Vapnik 1995], *Nearest Centroid* [McIntyre and Blashfield 1980], *K-nearest neighbor* (KNN) [Fix and Hodges Jr 1951], *Decision Tree* [Quinlan 1986], *Random Forest* [Ho 1995], *Artificial Neural Network* (ANN) [Vemuri 1988], *Perceptron* [Rosenblatt 1957], *MultiLayer Perceptron* (MLP) [Rumelhart et al. 1985], *Convolutional Neural Network* (CNN) [LeCun et al. 1989] com *Tensorflow* [Abadi et al. 2016], ResNet [He et al. 2016], VGG16 [Simonyan and Zisserman 2014].

Atualmente existem muitos *surveys* relacionados a análise e classificação de *malware*, mas nenhum aplica especificamente análise de texturas para tal finalidade. [Yu et al. 2016] mostram artigos que utilizam *Machine Learning* e visualização para detecção de intrusão. Apesar de utilizar *Machine Learning* para classificar *malware*, são aplicados em cenários diferentes, onde os autores não se preocupam com o tipo de *malware*, apenas em identificar anomalias na rede. [Gandotra et al. 2014] fizeram um *survey* para análise e classificação de *malware* cujo foco é na análise estática e dinâmica (texturas e visualização são apenas mencionados). [Wagner et al. 2015] realizaram um le-

vantamento de pesquisas que utilizam visualização para análise de *malware*. Nesse caso são exibidas outras estratégias de análise de *malware*, não especificamente a de texturas e não é considerada a classificação em si.

Foi apresentado um *survey* com técnicas de classificação de texturas em [Thakare et al. 2013], porém sem aplica-las ao problema do *malware* especificamente, semelhante ao *survey* de [Nanni et al. 2012], que também trabalha com classificação de imagens, mas usando descritor de texturas LBP. A classificação de *malware* por análise de texturas é uma abordagem relativamente nova que tem atingido boas taxas de acerto e precisão, além de ser rápida e agnóstica a sistema operacional [Nataraj et al. 2011a].

3. Metodologia

Para seleção dos trabalhos, foi feita uma revisão sistemática, baseada no modelo proposto por [Sampaio and Mancini 2007], com o objetivo de avaliar técnicas baseadas em análise de texturas para classificação de famílias de *malware*. A busca foi realizada utilizando as bases de dados eletrônicas *Google Scholar* e *Scopus*, as quais foram consultadas a partir de 2009 usando as seguintes palavras-chave: *malware classification* AND *texture analysis* AND *malware images* AND *visualization*. Optou-se por utilizar apenas artigos em inglês e com acesso gratuito ou disponibilizado pela instituição de ensino. Todos os artigos avaliados foram publicados entre janeiro de 2009 e julho de 2018, pois apesar de [Nataraj et al. 2011a] afirmarem ter proposto uma abordagem nova e completamente diferente de analisar *malware*, estendeu-se a busca a dois anos anteriores para verificar se não havia artigos com a mesma proposta.

Foi dado foco em artigos de caráter experimental quanto a classificação de *malware* em famílias, restringindo-se àqueles cuja análise da amostra é feita através da conversão do binário para texturas em escala de cinzas. Foram considerados apenas os experimentos tendo como desfecho a acurácia da classificação com amostras de no mínimo cinco mil exemplares. Não foram utilizados experimentos com apenas detecção ou análise de *malware* e, visando a qualidade metodológica dos estudos, foram excluídos artigos que traziam informações repetidas. A pesquisa inicial identificou 573 publicações, porém, após a análise e seleção de acordo com as especificações mencionadas anteriormente, restaram 17 avaliados neste artigo. Na Figura 1, pode-se ver o aumento nas publicações usando análise por texturas, indicando que esta pode ser uma boa estratégia. E a Figura 2 mostra que o número de diferentes autores publicando ao longo dos anos também tem aumentado, ou seja, novos pesquisadores têm demonstrado interesse neste tipo de análise.

4. Técnicas de Classificação de *Malware* baseadas em Texturas

A utilização da análise de texturas para classificação de *malware* foi proposta pela primeira vez em [Nataraj et al. 2011a]. Os autores usavam um descritor de texturas GIST como entrada do classificador, o qual apresentou resultado melhor do que outros descritores globais (HTD e CLD), e que também foi o descritor utilizado em outros trabalhos [Nataraj et al. 2011b] [Nataraj 2015] [Kosmidis and Kalloniatis 2017] [Luo and Lo 2017]. Seguindo a mesma ideia, [Makandar and Patrot 2015a] utilizam como descritor o GWT em conjunto com GIST, pois a escolha do descritor de textura é de fundamental importância para a correta classificação. Já [Makandar and Patrot 2015b] e [Makandar and Patrot 2018] utilizam GWT como único descritor, porém não atingem

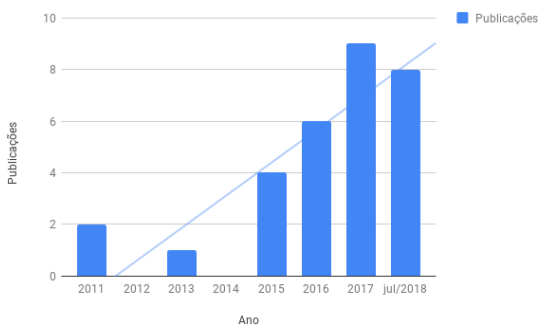

Figura 1. Número de publicações que utilizam análise de texturas de *malware* por ano.

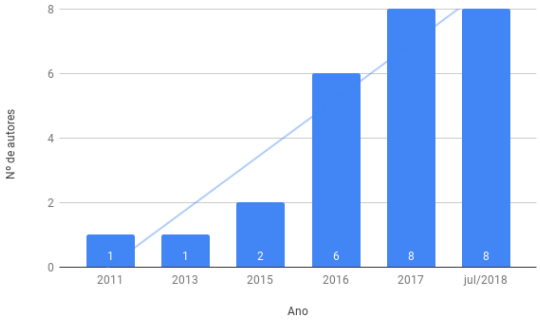

Figura 2. Número de autores diferentes com publicações que utilizam análise de texturas de *malware* por ano.

uma acurácia de classificação tão alta. [Makandar and Patrot 2016] propõem a utilização do DWT em conjunto com GIST, aumentando a taxa de acerto, enquanto que o DWT é utilizado sozinho por [Makandar and Patrot 2017a] e [Makandar and Patrot 2017b]. [Luo and Lo 2017] decidem utilizar um descritor local para evitar erro de classificação nos casos de realocação de seções ou quando se é adicionado grande quantidade de dados redundantes, problema já sugerido em [Nataraj et al. 2011b], mostrando que mesmo com diferentes classificadores, o descritor local apresenta melhores acurácia.

Outro fator importante que interfere diretamente nos resultados é a escolha do classificador. [Nataraj et al. 2011a], [Nataraj et al. 2011b], [Nataraj 2015], [Makandar and Patrot 2016], [Luo and Lo 2017], [Makandar and Patrot 2017a] e [Makandar and Patrot 2018] optam pelo KNN que, apesar de ser um classificador bastante simples (assume que todas as instâncias correspondem a pontos no espaço e relaciona-as com suas vizinhas [Mitchell 1997]), apresenta uma boa taxa de acurácia. KNN atingiu o melhor resultado dentre os demais classificadores utilizados para texturas de *malware* [Makandar and Patrot 2016]. [Makandar and Patrot 2015b], [Luo and Lo 2017], [Makandar and Patrot 2017a], [Makandar and Patrot 2017b] e [Makandar and Patrot 2018] também utilizam o classificador SVM, que é efetivo em espaços de grande dimensão e apresentou resultados bastante significativos, alcançando a melhor acurácia dentre as pesquisas apresentadas em [Makandar and Patrot 2017a], o mesmo alcançado anteriormente utilizando KNN. [Kosmidis and Kalloniatis 2017] fazem uma comparação entre diferentes classificadores, apresentando não só a acurácia de classificação, mas o tempo médio de treino e teste de cada um deles. Redes Neurais Artificiais e suas variações foram apresentadas em [Makandar and Patrot 2015a], [Singh 2017], [Rezende et al. 2017], [Rezende et al. 2018], [Yakura et al. 2018] e [Kabanga and Kim 2018], mostrando que as pesquisas mais recentes têm apostado em sua utilização para classificação, pois apresentam altas taxas de acurácia e por vezes são mais rápidas que outras abordagens, como o uso de *TensorFlow* e CNN [Luo and Lo 2017].

A Tabela 1 exibe o estado da arte em classificação de *malware* por análise de texturas, diferenciando os trabalhos por descritor, classificador, pré-processamento da imagem por redimensionamento (*resize*), acurácia alcançada por cada técnica e *dataset* utilizado. Com essas informações extraídas dos artigos selecionados, é possível identifi-

car as técnicas mais aplicadas e que têm apresentado melhor resultado. Na próxima seção é feita uma comparação para categorizar esses artigos.

Tabela 1. Comparação de técnicas usadas para classificação de *malware* usando análise de texturas (*n/i*: não informado pelo autor; ✗: descritor não necessário.)

Referência	*Resize*	Descritor	Classificador	Acurácia (%)	*Dataset*
[Nataraj et al. 2011a]	*n/i*	GIST	KNN	98,00	Malimg
[Nataraj et al. 2011b]	64x64	GIST	KNN	95,14 97,57 72,80	Host-Rx Malhuer VX Heaven
[Makandar and Patrot 2015a]	64x64	GWT + GIST	ANN	96,35	Malheur
[Makandar and Patrot 2015b]	*n/i*	GWT	SVM	89,68	Malheur
[Nataraj 2015]	64x64	GIST	KNN	97,40 98,37 97,40 83,27	Malimg Malheur MalGenome VXShare
[Makandar and Patrot 2016]	*n/i*	DWT, GIST	KNN	98,88	Malimg
[Kosmidis and Kalloniatis 2017]	32x32	GIST	Decision Tree Nearest Centroid SGD Perceptron MLP Random Forest	88,00 85,60 87,00 90,50 87,80 91,60	Malimg
[Yue 2017]	*n/i*	✗	CNN	98,63	Malimg
[Luo and Lo 2017]	*n/i*	LBP GIST	CNN (TensorFlow) SVM KNN CNN (TensorFlow) SVM KNN	93,17 87,88 85,93 87,88 81,23 82,83	Malimg
[Makandar and Patrot 2017a]	64x64	DWT	KNN SVM	98,84 98,88	Malimg
[Makandar and Patrot 2017b]	256x256	DWT	SVM	91,05 92,53	Malheur Malimg
[Singh 2017]	32x32	✗	CNN CNN (ResNet) CNN (ResNet)	95,24 98,21 96,08	Malshare + VirusShare + VirusTotal. Malimg
[Rezende et al. 2017]	224x224	✗	CNN (ResNet)	98,62	Malimg
[Rezende et al. 2018]	224x224	✗	CNN (VGG16)	92,97	VirusSign
[Yakura et al. 2018]	64x64	*n/i*	CNN	49,03	VX Heaven
[Makandar and Patrot 2018]	128x128	GWT	KNN SVM	89,11 75,11	Malimg
[Kabanga and Kim 2018]	128x128	*n/i*	CNN	98,00	Malimg

5. Categorização e Comparação da Literatura

Como explicado na Seção 2, um classificador recebe como entrada algumas características do exemplar a ser avaliado, normalmente extraídas por um descritor de texturas. O objetivo é determinar a qual família uma amostra pertence, tornando a escolha do descritor de suma importância para a classificação. A Tabela 1 mostra que o descritor mais

comumente utilizado é o GIST. [Nataraj 2015] fez uma comparação entre alguns descritores globais (GIST, HTD e CLD), onde o primeiro apresentou melhores resultados. Já [Luo and Lo 2017] fez uma comparação com o descritor LBP e o GIST, onde este último apresentou resultado inferior ao descritor local. Em outras pesquisas o GIST é utilizado em conjunto com outros descritores, podendo significar que este possui características importantes para classificação. Cabe ressaltar que algoritmos baseados em *deep learning* não necessitam de descritor da textura, pois o próprio classificador seleciona as características da imagem mais importantes.

A análise dos trabalhos da área deixa claro que o uso de diferentes descritores interfere na taxa de acerto da classificação. É possível perceber isso comparando os resultados de [Nataraj et al. 2011a] e [Makandar and Patrot 2017a], nos quais os autores fazem uso do mesmo classificador (KNN) e conjunto de dados, porém alcançam taxas de acurácia distintas, pois se diferenciam no descritor. Isso pode ser também constatado na comparação feita por [Luo and Lo 2017] que avalia dois descritores em diferentes classificadores, mostrando que alterando-se o descritor, tem-se melhor acurácia em todos os classificadores testados. Apesar de ser difícil realizar uma comparação direta entre todos os trabalhos (diferentes *datasets* e redimensionamentos), a Figura 3 mostra a acurácia alcançada por classificadores que utilizam descritor GIST, enquanto que a Figura 4 mostra a acurácia obtida com outros descritores.

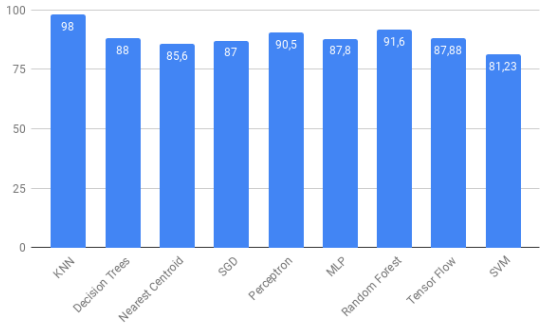

Figura 3. Acurácia de classificação utilizando descritor GIST em diferentes classificadores.

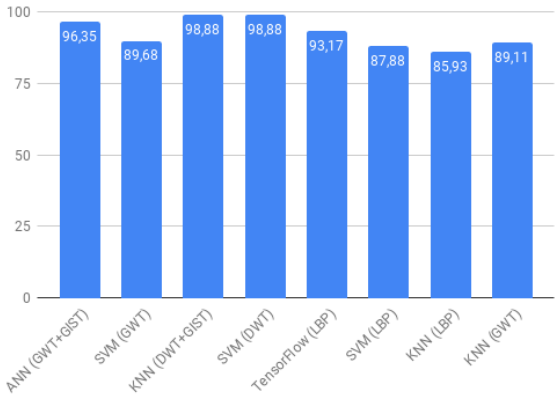

Figura 4. Acurácia de classificação utilizando outros descritores em diferentes classificadores.

Os classificadores cujo descritor é o GIST utilizaram o mesmo *dataset* em todos os casos (Figura 3), porém há diferenças quanto ao redimensionamento da imagem, o que pode ter interferido nos resultados. Já a classificação apresentada na Figura 4 referente aos demais descritores exibe resultados um pouco mais difíceis de comparar, pois os autores fazem uso de *datasets* distintos em alguns casos e com diferentes redimensionamentos.

Ainda, como já mencionado, alguns autores não utilizam descritor de texturas, pois o próprio classificador faz a seleção das características. Na Figura 5, exibe-se a acurácia das redes neurais convolucionais (CNN) propostas na literatura conforme sua arquitetura e para *datasets* distintos. As CNNs com mais camadas apresentaram melhores taxas de acerto, porém problemas de degradação e desaparecimento de gradientes costumam aparecer conforme aumenta-se a profundidade da rede neural [Singh 2017], portanto

é necessário utiliza-las com cautela. Novamente há uma dificuldade em comparar os resultados devido ao redimensionamento inicial da imagem.

Como visto, na etapa de pré-processamento da imagem, alguns autores fazem o redimensionamento da mesma, deixando-a quadrada. [Nataraj et al. 2013] definem esse valor como 64x64, pois um valor menor não retorna uma assinatura significativa e um maior aumenta a complexidade computacional. Porém, esse valor é escolhido empiricamente e não há um consenso sobre o melhor valor a ser fixado. A Figura 6 mostra a diferença da pior e melhor acurácia obtida na classificação por texturas com redimensionamento de imagem, desconsiderando-se descritor e classificador utilizados.

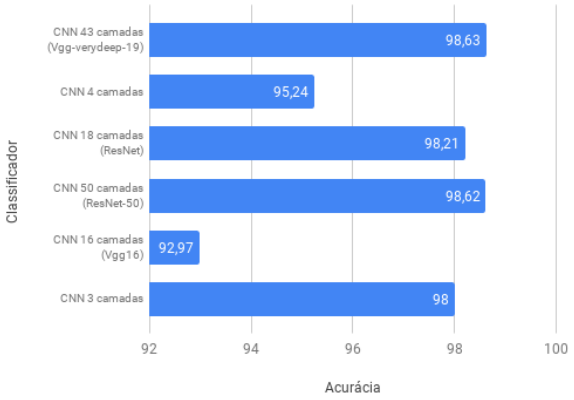

Figura 5. Acurácia obtida para diferentes arquiteturas de CNN.

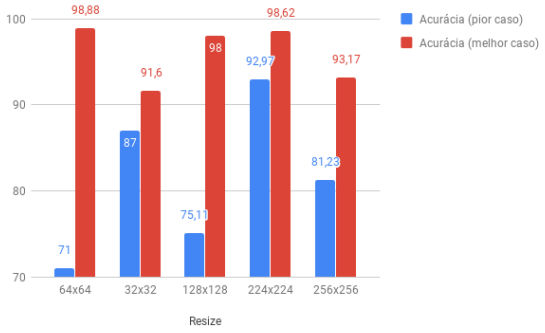

Figura 6. Melhor e pior acurácia obtidas em cada redimensionamento.

Levando-se em conta só os resultados obtidos com o redimensionamento da imagem, apesar da melhor acurácia ser o de 64x64, talvez o mais prudente seria utilizar um redimensionamento por 224x224, dada a menor variação e mantendo alta taxa de acerto em todos os casos. A utilização de diferentes *datasets* dificulta a comparação real das técnicas apresentadas. Foram identificados oito *datasets* utilizados na literatura, mas o mais usado é o Malimg ([Nataraj et al. 2011a]), que possui 9342 amostras de 25 famílias de *malware* já convertidas em textura. A Tabela 2 mostra as informações básicas de cada *dataset* conforme a literatura e a acurácia obtida pelos autores em cada base.

Tabela 2. *Datasets* utilizados na literatura para classificação de *malware* em famílias.

Nome do *Dataset*	**Exemplares**	**Famílias**	**Acurácia** (%)
Host-Rx	393	6	95,14
Malheur	3.131	24	89,68 a 98,37
VX Heaven	63.002	531	72,8
Malimg	9.342	25	75,11 a 98,88
MalGenome	1.094	13	97,4
VXShare	568	8	83,27
Singh 2017 (VirusShare, VirusTotal, Malshare)	44.945	20	95,24 a 98,21
VirusSign	10.136	20	92,97

Nota-se na Tabela 2 que, para um *dataset* com uma grande quantidade de famílias, a taxa de acerto classificação diminui. Porém, como em outros casos, o classificador e

descritor utilizados podem também ter interferido nesse resultado. Para uma comparação justa, seria importante usar a mesma técnica para todos os *datasets*.

6. Conclusão e Trabalhos Futuros

Classificação de *malware* em famílias é um problema que tenta ser solucionado há muitos anos e dentre diversas abordagens utilizadas na literatura, o uso de análise de texturas tem crescido nos últimos anos. Neste artigo, apresentou-se uma revisão da literatura apontando quais são as abordagens utilizadas para classificação de *malware* baseadas na transformação do binário em textura, mostrando os diferentes tipos de descritores e classificadores que apresentam boas taxas de acurácia.

Os trabalhos aqui apresentados não puderam ser diretamente comparados em muitos casos devido a utilização de diferentes *datasets* e se diferenciar não só pelo classificador, mas também por descritor e pré-processamento de imagem. Para identificar técnicas mais apropriadas para obter melhor acurácia de classificação, deixou-se como trabalhos futuros a reimplementação dos algoritmos apresentados na literatura e sua aplicação em um *dataset* comum, variando-se cada aspecto (descritor e redimensionamento) a partir disso.

Referências

Abadi, M., Barham, P., Chen, J., Chen, Z., Davis, A., Dean, J., Devin, M., Ghemawat, S., Irving, G., Isard, M., et al. (2016). Tensorflow: a system for large-scale machine learning. In *OSDI*, volume 16, pages 265–283.

Bannour, H., Hlaoua, L., and el Ayeb, B. (2009). Survey of the adequate descriptor for content-based image retrieval on the web: Global versus local features. In *CORIA*, pages 445–456.

Cortes, C. and Vapnik, V. (1995). Support-vector networks. *Machine Learning*, 20(3):273–297.

Damodaran, A., Troia, F. D., Visaggio, C. A., Austin, T. H., and Stamp, M. (2017). A comparison of static, dynamic, and hybrid analysis for malware detection. *Journal of Computer Virology and Hacking Techniques*, 13(1):1–12.

Fix, E. and Hodges Jr, J. L. (1951). Discriminatory analysis-nonparametric discrimination: consistency properties. Technical report, California Univ Berkeley.

Gandotra, E., Bansal, D., and Sofat, S. (2014). Malware analysis and classification: A survey. *Journal of Information Security*, 5(02):56.

He, K., Zhang, X., Ren, S., and Sun, J. (2016). Deep residual learning for image recognition. In *Proceedings of the IEEE conference on computer vision and pattern recognition*, pages 770–778.

Ho, T. K. (1995). Random decision forests. In *Document analysis and recognition, 1995., proceedings of the third international conference on*, volume 1, pages 278–282. IEEE.

Idika, N. and Mathur, A. P. (2007). A survey of malware detection techniques. *Purdue University*, 48.

Kabanga, E. K. and Kim, C. H. (2018). Malware images classification using convolutional neural network. *Journal of Computer and Communications*, 6(01):153–158.

Kosmidis, K. and Kalloniatis, C. (2017). Machine learning and images for malware detection and classification. In *Proceedings of the 21st Pan-Hellenic Conference on Informatics*, PCI 2017, pages 5:1–5:6, New York, NY, USA. ACM.

LeCun, Y., Boser, B., Denker, J. S., Henderson, D., Howard, R. E., Hubbard, W., and Jackel, L. D. (1989). Backpropagation applied to handwritten zip code recognition. *Neural computation*, 1(4):541–551.

Luo, J. and Lo, D. C. (2017). Binary malware image classification using machine learning with local binary pattern. In *2017 IEEE International Conference on Big Data (Big Data)*, pages 4664–4667.

Makandar, A. and Patrot, A. (2015a). Malware analysis and classification using artificial neural network. In *2015 International Conference on Trends in Automation, Communications and Computing Technology*.

Makandar, A. and Patrot, A. (2015b). Malware image analysis and classification using support vector machine. *International Journal of Trends in Computer Science and Engineering*, 4(5):01–03.

Makandar, A. and Patrot, A. (2016). An approach to analysis of malware using supervised learning classification. In *International Conference on Recent Trends in Engineering, Science Technology - (ICRTEST 2016)*, pages 1–5.

Makandar, A. and Patrot, A. (2017a). Malware class recognition using image processing techniques. In *2017 International Conference on Data Management, Analytics and Innovation (ICDMAI)*, pages 76–80.

Makandar, A. and Patrot, A. (2017b). Wavelet statistical feature based malware class recognition and classification using supervised learning classifier. *Oriental Journal of Computer Science and Technology*, 10(2):400–406.

Makandar, A. and Patrot, A. (2018). Trojan malware image pattern classification. In Guru, D. S., Vasudev, T., Chethan, H., and Kumar, Y. S., editors, *Proceedings of International Conference on Cognition and Recognition*, pages 253–262, Singapore. Springer Singapore.

Manjunath, B. S. and Ma, W.-Y. (1996). Texture features for browsing and retrieval of image data. *IEEE Transactions on pattern analysis and machine intelligence*, 18(8):837–842.

Manjunath, B. S., Ohm, J.-R., Vasudevan, V. V., and Yamada, A. (2001). Color and texture descriptors. *IEEE Transactions on circuits and systems for video technology*, 11(6):703–715.

McIntyre, R. M. and Blashfield, R. K. (1980). A nearest-centroid technique for evaluating the minimum-variance clustering procedure. *Multivariate Behavioral Research*, 15(2):225–238.

Mitchell, T. M. (1997). *Machine Learning*. McGraw-Hill, New York.

Nanni, L., Lumini, A., and Brahnam, S. (2012). Survey on lbp based texture descriptors for image classification. *Expert Systems with Applications*, 39(3):3634 – 3641.

Nataraj, L. (2015). *A Signal Processing Approach To Malware Analysis*. PhD thesis, University of California, Santa Barbara, CA, USA.

Nataraj, L., Karthikeyan, S., Jacob, G., and Manjunath, B. S. (2011a). Malware images: Visualization and automatic classification. In *Proceedings of the 8th International Symposium on Visualization for Cyber Security*, VizSec '11, pages 4:1–4:7, New York, NY, USA. ACM.

Nataraj, L., Kirat, D., Manjunath, B., and Vigna, G. (2013). Sarvam: Search and retrieval of malware. In *Proceedings of the Annual Computer Security Conference (ACSAC) Worshop on Next Generation Malware Attacks and Defense (NGMAD)*.

Nataraj, L., Yegneswaran, V., Porras, P., and Zhang, J. (2011b). A comparative assessment of malware classification using binary texture analysis and dynamic analysis. In *Proceedings of the 4th ACM Workshop on Security and Artificial Intelligence*, AISec '11, pages 21–30, New York, NY, USA. ACM.

Ojala, T., Pietikainen, M., and Maenpaa, T. (2002). Multiresolution gray-scale and rotation invariant texture classification with local binary patterns. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 4(7):971–987.

Oliva, A. and Torralba, A. (2001). Modeling the shape of the scene: A holistic representation of the spatial envelope. *International Journal of Computer Vision*, 42(3):145–175.

Quinlan, J. R. (1986). Induction of decision trees. *Machine learning*, 1(1):81–106.

Rezende, E., Ruppert, G., Carvalho, T., Ramos, F., and de Geus, P. (2017). Malicious software classification using transfer learning of resnet-50 deep neural network. In *2017 16th IEEE International Conference on Machine Learning and Applications (ICMLA)*, pages 1011–1014.

Rezende, E., Ruppert, G., Carvalho, T., Theophilo, A., Ramos, F., and Geus, P. d. (2018). Malicious software classification using vgg16 deep neural network's bottleneck features. In Latifi, S., editor, *Information Technology - New Generations*, pages 51–59, Cham. Springer International Publishing.

Robbins, H. and Monro, S. (1985). A stochastic approximation method. In *Herbert Robbins Selected Papers*, pages 102–109. Springer.

Rosenblatt, F. (1957). *The perceptron, a perceiving and recognizing automaton Project Para*. Cornell Aeronautical Laboratory.

Rumelhart, D. E., Hinton, G. E., and Williams, R. J. (1985). Learning internal representations by error propagation. Technical report, California Univ San Diego La Jolla Inst for Cognitive Science.

Sampaio, R. and Mancini, M. (2007). Estudos de revisão sistemática: um guia para síntese criteriosa da evidência científica. *Revista brasileira de fisioterapia*, 11(1):83–89.

Sathya, R. and Abraham, A. (2013). Comparison of supervised and unsupervised learning algorithms for pattern classification. *International Journal of Advanced Research in Artificial Intelligence*, 2(2):34–38.

Shensa, M. J. (1992). The discrete wavelet transform: wedding the a trous and mallat algorithms. *IEEE Transactions on Signal Processing*, 40(10):2464–2482.

Simonyan, K. and Zisserman, A. (2014). Very deep convolutional networks for large-scale image recognition. *arXiv preprint arXiv:1409.1556*.

Singh, A. (2017). Malware classification using image representation. Master's thesis, Department of Computer Science and Engineering - Indian Institute of Technology Kanpur, Kanpur, UP, India.

Symantec (2017). 2017 internet security threat report. `https://digitalhubshare.symantec.com/content/dam/Atlantis/campaigns-and-launches/FY17/Threat\%20Protection/ISTR22_Main-FINAL-JUN8.pdf?aid=elq_`. Acessado em 25/07/2017.

Thakare, V. S., Patil, N. N., and Sonawane, J. S. (2013). Survey on image texture classification techniques. *International Journal of Advancements in Technology*, 4(1):97–104.

Vemuri, V., editor (1988). *Artificial Neural Networks: Theoretical Concepts*. IEEE Computer Society Press, Los Alamitos, CA, USA.

Wagner, M., Fischer, F., Luh, R., Haberson, A., Rind, A., Keim, D. A., and Aigner, W. (2015). A Survey of Visualization Systems for Malware Analysis. In Borgo, R., Ganovelli, F., and Viola, I., editors, *Eurographics Conference on Visualization (EuroVis) - STARs*. The Eurographics Association.

Yakura, H., Shinozaki, S., Nishimura, R., Oyama, Y., and Sakuma, J. (2018). Malware analysis of imaged binary samples by convolutional neural network with attention mechanism. In *Proceedings of the Eighth ACM Conference on Data and Application Security and Privacy*, CODASPY '18, pages 127–134, New York, NY, USA. ACM.

Yu, Y., Long, J., Liu, F., and Cai, Z. (2016). Machine learning combining with visualization for intrusion detection: A survey. In Torra, V., Narukawa, Y., Navarro-Arribas, G., and Yañez, C., editors, *Modeling Decisions for Artificial Intelligence*, pages 239–249, Cham. Springer International Publishing.

Yue, S. (2017). Imbalanced malware images classification: a CNN based approach. *CoRR*, abs/1708.08042.