VISUALISASI (CITRA GRAYSCALE) DAN KLASIFIKASI MALWARE MENGGUNAKAN METODE SUPPORT VECTOR MACHINE

TUGAS AKHIR
Program Studi Sistem Komputer
Jenjang S1

Oleh

Therio Anggara
09011281520112

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
2020

VISUALISASI (CITRA GRAYSCALE) DAN KLASIFIKASI MALWARE MENGGUNAKAN METODE *SUPPORT VECTOR MACHINE*

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

OLEH :

Therio Anggara

09011281520112

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
2020

LEMBAR PENGESAHAN

VISUALISASI (CITRA GRAYSCALE) DAN KLASIFIKASI MALWARE MENGGUNAKAN METODE *SUPPORT VECTOR MACHINE*

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh

Therio Anggara
09011281520112

Palembang, 31 Desember 2020

Mengetahui,

Ketua Jurusan Sistem Komputer

Dr. Ir. H. Sukemi, M.T.
NIP. 196612032006041001

Pembimbing Tugas Akhir

Deris Stiawan, M.T., Ph.D.
NIP. 197806172006041002

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada :

Hari : Kamis

Tanggal : 31 Desember 2020

Tim Penguji :

1.	**Ketua**	**: Kemahyanto Exaudi, M.T.**	
2.	**Sekretaris**	**: Sri Desy Siswanti, M.T.**	By dosi at 10:17:13, 06/01/2021
3.	**Anggota 1**	**: Ahmad Heryanto, M.T.**	

Mengetahui,

Ketua Jurusan Sistem Komputer

Dr. Ir. H. Sukemi, M. T.

NIP. 196612032006041001

HALAMAN PERNYATAAN

Yang bertanda tangan dibawah ini :

Nama	: Therio Anggara
NIM	: 09011281520112
Program Studi	: Sistem Komputer
Judul	: Visualisasi (Citra Grayscale) dan Klasifikasi Malware Menggunakan Metode *Support Vector Machine*

Menyatakan bahwa laporan Tugas Akhir saya merupakan hasil karya sendiri dan bukan hasil penjiplakan atau plagiat. Apabila ditemukan unsur penjiplakan atau plaiat dalam laporan Tugas Akhir ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya. Demikian, pernyataan ini saya buat dalam keadaan sadar dan tidak dipaksakan.

Palembang, 31 Desember 2020

Therio Anggara

NIM. 09011281520112

HALAMAN PERSEMBAHAN

“Terus Berusaha dan Mencoba”

Tugas Akhir ini saya persembahkan untuk :

- ***Kedua Orang Tua,Abang,Kakak Saya***
- ***Saudara seperjuangan, teman-teman Kelas SKC dan Angkatan 2015***
- ***Anggota Tim Khusus***
- ***Dosen Pembimbing dan Penguji***
- ***Jurusan Sistem Komputer***
- ***Almamaterku***

KATA PENGANTAR

Assalamu'alaikum Warahmatullahi Wabarakatuh

Puji dan syukur penulis panjatkan kehadirat Allah SWT, atas segala karunia dan rahmat-Nya sehingga penulis dapat menyelesaikan penyusunan Proposal Tugas Akhir ini dengan judul "Visualisasi (Citra Grayscale) dan Klasifikasi Malware Menggunakan Metode Support Vector Machine".

Dalam laporan ini penulis menjelaskan mengenai Visualisasi malware ke dalam citra grayscale dan mengklasifikasikannya dengan *Support Vector Machine* . Penulis berharap tulisan ini dapat bermanfaat bagi orang banyak, dan menjadi tambahan bahan bacaan bagi yang tertarik meneliti tentang pengklasifikasian malware.

Pada penyusunan proposal tugas akhir ini, tidak terlepas dari bantuan, bimbingan serta dukungan dari berbagai pihak. Oleh karena itu, pada kesempatan ini penulis mengucapkan rasa syukur dan terima kasih kepada yang terhormat :

1. Allah SWT, yang telah memberikan kemudahan, kesehatan, serta kesempatan dalam pelaksanaan pembuatan Tugas Akhir ini.
2. Papa, Mama, Abang, Kakak,Ayuk yang telah memberikan dukungan dan nasehat-nasehat serta motivasi selama ini. Terima kasih atas dukungan baik berupa moral, material, maupun spiritual.
3. Bapak Jaidan Jauhari, S.Pd., M.T selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya
4. Bapak Dr. Ir. H. Sukemi, M.T. selaku Ketua Jurusan Sistem Komputer Fakutas Ilmu Komputer Universitas Sriwijaya
5. Bapak Deris Stiawan, M.T., Ph.D. selaku Pembimbing Tugas Akhir Penulis di Jurusan Sistem Komputer. Terima kasih karena telah meluangkan waktunya untuk membimbing penulis dalam menyelesaikan tugas akhir ini serta telah memberikan bimbingan dan nasehat selama perkuliahan.
6. Bapak Ahmad Heryanto, M.T. selaku Dosen Pembimbing Akademik

7. Seluruh Dosen Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya.
8. Teman-teman seperjuangan Sistem Komputer angkatan 2015 dan anak-anak SKC khususnya yang selalu membersamai selama perkuliahan ini.
9. Serta semua pihak yang telah membantu baik moril maupun materil yang tidak dapat disebutkan satu persatu dalam penyelesaian tugas akhir ini. Terima kasih banyak semuanya.

Penulis menyadari bahwa masih terdapat banyak kekurangan dalam penulisan Tugas Akhir ini, baik dari materi maupun teknik penyajiannya, mengingat kurangnya pengetahuan dan pengalaman penulis. Untuk itu, penulis mengharapkan adanya kritik dan saran yang membangun agar dapat memperbaiki kekurangan-kekungan tersebut kedepannya nanti.

Akhir kata dengan segala keterbatasan, penulis berharap semoga penulisan Tugas Akhir ini dapat menjadi tambahan wawasan dan ilmu pengetahuan bagi mahasiswa yang memerlukan khususnya mahasiswa Fakultas Ilmu Komputer Universitas Sriwijaya secara langsung ataupun tidak langsung sebagai sumbangan pikiran dalam peningkatan mutu pembelajaran.

Palembang, Desember 2020
Penulis

Therio Anggara

Visualisasi (Citra Grayscale) dan Klasifikasi Malware Menggunakan Metode *Support Vector Machine*

Therio Anggara (09011281520112)

Jurusan Sistem Komputer, Fakultas Ilmu Komputer

Universitas Sriwijaya

Email: anggaratherio@gmail.com

ABSTRAK

Penelitian ini berfokus pada proses visualisasi data tangkapan malware ke dalam citra grayscale, dari citra grayscale tersebut terdapat pola perulangan,pola tersebut akan diambil fiturnya dengan menggunakan Gray Level Coocurrence Matrix dengan sudut 0, 45, 90, 135 dengan atribut dissimilarity, correlation, homogeneity, contrast, ASM, energy. Fitur yang didapat akan dilakukan pemberian label dilanjutkan dengan proses training data,dimana sistem akan mempelajari data training secara rinci, setelah sistem memepelajari data training akan dilakukan proses uji dengan mengklasifikasikan malware yang ada ke familinya masing-masing dengan menggunakan metode *Support Vector Machine*.

Kata Kunci : *Support Vector Machine, Gray Level Coocurrence Matrix* , Machine learning, Visualisasi

Visualization (Grayscale Image) and Malware Classification Using Support Vector Machine Method

Therio Anggara (09011281520112)

Department of Computer Engineering, Faculty of Computer Science

Sriwijaya University

Email: anggaratherio@gmail.com

ABSTRACT

This research is based on the process of visualizing malware capture data into a grayscale image, from the grayscale image there is a repeating pattern, the pattern will be taken using the Gray Level Coocurrence Matrix with angles 0, 45, 90, 135 with attributes of dissimilarity, correlation, homogeneity, contrast, ASM, energy. The features obtained will be carried out by presenting labels with the training data process, where the system will study the training data in detail, after the system learns the training data, the test process will be carried out by classifying the existing malware into their respective families using the Support Vector Machine method.

Keywords **:** *Support Vector Machine, Gray Level Coocurrence Matrix* , Machine learning, Visualization

DAFTAR ISI

Halaman

BAB II TINJAUAN PUSTAKA

BAB III METODOLOGI PENELITIAN

DAFTAR GAMBAR

Halaman

DAFTAR TABEL

Halaman

BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan Malware pada saat ini telah menjadi perhatian khusus bagi penggiat teknologi di berbagai penjuru dunia, hal ini tidak lepas dari perkembangan malware yang begitu pesat, malware merupakan ancaman utama pada keamananan internet sampai saat ini [1]. Pada Umumnya malware yang ada diciptakan untuk melakukan serentetan tindakan illegal yang merugikan *end-user*. Mencuri, membebani sistem, merusak data yang tersimpan di media penyimpanan, merupakan contoh nyata bahwa malware yang ada tidak bisa dianggap sepele. Hal ini juga yang banyak mendorong orang untuk mempelajari, memahami behavior dari malware itu sendiri.

Berkembangnya malware yang begitu cepat ini juga berbanding lurus dengan kebutuhan untuk mengelola data dalam jumlah besar yang harus dievaluasi, data yang lebih besar ini disebabkan oleh malware yang semakin "pintar", malware-malware yang ada mencoba untuk menghindari deteksi, malware dengan "family" yang sama,dengan behavior yang sama,secara konstan memodifikasi dan menyamarkan diri,sehingga muncul sebagai banyak file yang berbeda satu sama lain [2]. Merupakan sebuah tantangan bagi para pengembang anti-malware untuk memperbarui kemampuan yang diusung dalam setiap anti-malware yang ada, guna memberikan kenyamanan kepada pengguna.

Klasifikasi malware, dilakukan untuk mengelompokkan malware ke dalam kelompoknya masing-masing sehingga dapat memudahkan dalam menganalisa lebih lanjut data malware yang ada, ada berbagai cara yang dapat dilakukan untuk mengklasifikasi malware,salah satunya ialah memanfaatkan teknik pengolahan citra untuk mengubah binari malware ke dalam sebuah citra grayscale yang kemudian diklasifikasikan menggunakan machine learning sesuai dengan family dari malware itu sendiri .

Dalam pengklasifikasian algoritma support vector machine merupakan salah satu algoritma yang sering digunakan. Support Vector Machine pada dasarnya digunakan untuk mempelajari fungsi linear threshold function,tetapi dengan

beberapa perubahan atau modifikasi kernel, Support Vector Machine dapat juga untuk mempelajari berbagai fungsi.

1.2 Tujuan

Pada penelitian ini terdapat beberapa tujuan, antara lain:

1. Memvisualisasikan binari malware kedalam sebuah citra grayscale.
2. Memahami penerapan *Gray Level Coocurrence Matrix (GLCM)* pada ekstraksi fitur grayscale
3. Menerapkan algoritma *Support Vector Machine* untuk klasifikasi malware.
4. Untuk menganalisis bagaimana tingkat keakurasian *Support Vector Machine* (SVM) dalam pengklasifikasian malware yang sudah diubah terlebih dahulu citra grayscale

1.3 Manfaat

1. Dapat memahami dan juga penerapan *Gray Level Coocurrence Matrix (GLCM)* pada.
2. Dapat memahami penerapan algoritma *Support Vector Machine* pada prpengklasifikasian malware
3. Penelitian ini dapat dijadikan bahan rujukan pada penelitian selanjutnnya.

1.4 Rumusan Masalah

1. Dapatkah citra grayscale diambil fiturnya mneggunakan *Gray Level Coocurrence Matrix (GLCM)* ?
2. Apakah keakurasian dari sistem klasifikasi *Support Vector Machine* dalam klasifikasi malware berdasarkan citra grayscale sudah cukup baik?

1.5 Batasan Masalah

1. Penelitian ini dilakukan dengan jumlah malware yang tidak terlalu banyak, semakin banyak malware yang digunakan maka hasil semakin baik
2. Penelitian dilakukan dalam 2 tahapan, yaitu visualisasi dan klasifikasi.
3. Penggunaan *Support Vector Machine* sebagai pendekatan terhadap pengklasifikasian malware terdapat batasan, yaitu penggunaan kernel.

1.6 Metodelogi Penelitian

Metodelogi pada penelitian ini terdiri dari beberapa tahap, tahapan-tahapan tersebut ialah sebagai berikut:

1. Studi Pustaka atau Literatur

   Tahapan awal yaitu dengan mulai mencari dan memilih literatur yang sesuai dan dapat dijadikan sebagai referensi, hal ini dilakukan untuk mempermudah dalam pengerjaan tugas akhir yang dilakukan.

2. Konsultasi

   Tahapan selanjutnya atau tahapan kedua adalah konsultasi, di sini meupakan tahapan dimana orang-orang yang memiliki kemampuan atau pengetahuan yang sesuai dengan topik penelitian akan dimintai saran atau pendapat oleh peneliti.

3. Pengumpulan Data

   Tahapan ketiga dilakukan dengan mengumpulkan data yang akan menjadi bahan penelitian, data yang digunakan di sini adalah dataset malware dari Microsoft, dataset tersebut merupakan hasil tangkapan dari antimalware dari Microsoft

4. Pengolahan Data

Tahapan keempat dilakukan proses olah data dengan mengolah data malware yang ada guna dikonversi ke citra grayscale serta menerapkan algoritma *Support Vector Machine* pada pengklasifikasian malware.

5. Analisa

Tahapan kelima merupakan tahapan dimana hasil dari pengolahan data akan dianalisa,hal-hal penting yang ada akan dikaji guna mendapatkan kesimpulan

6. Kesimpulan dan Saran

Tahap keenam merupakan tahapan terakhir,setelah mengkaji hal-hal penting yang terdapat pada penelitian yang ada, maka akan didapatkan sebuah kesimpulan yang mewakili keseluruhan penelitian, serta saran yang dapat dijadikan referensi bagi yang tertarik untuk meneliti lebih lanjut

Daftar Pustaka

[1]. Ni, S., Qian, Q., & Zhang, R. (2018). Malware identification using visualization images and deep learning. *Computers and Security*, *77*, 871–885.

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

[3]. Sathya, R., & 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.

[4]. Joachims, T. (1998). Text categorization with support vector machines: Learning with many relevant features.*Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes Bioinformatics)*,*1398*,137–142.

[5]. Tunsaringkarn, T., Tungjaroenchai, W., & Siriwong, W. (2013). May 2013 Online Print Version International Journal of Scientific and Research Publications Edition. *International Journal of Scientific and Research Publications*, *3*(5), 1–8.

[6] I. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning*. The MIT Press, 2016.

[7]. Widodo, R., Widodo, A. W., & Supriyanto, A. (2018). Pemanfaatan Ciri Gray Level Co-Occurrence Matrix (GLCM) Citra Buah Jeruk Keprok (Citrus reticulata Blanco) untuk Klasifikasi Mutu. *Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer*, *2*(11), 5769–5776.

[8]. Zhang, Y., Ren, W., Zhu, T., & Ren, Y. (2019). SaaS: A situational awareness and analysis system for massive android malware detection. *Future Generation Computer Systems*, *95*, 548–559.

[9]. Nataraj, L., Karthikeyan, S., Jacob, G., & Manjunath, B. S. (2011). Malware images: Visualization and automatic classification. *ACM International Conference Proceeding Series*.

[10]. Abdelmounaime, S., & Dong-Chen, H. (2013). New Brodatz-Based Image Databases for Grayscale Color and Multiband Texture Analysis. *ISRN Machine Vision*, *2013*, 1–14.

[11]. Lamdompak Sistem Komputer, E. S., & Ilmu Komputer, F. (2016). *Klasifikasi Malware Trojan Ransomware Dengan Algoritma Support Vector Machine (SVM)*. *2*(1), 122–127.

[12]. J.-Y. Wang, "Support Vector Machines (SVM) in bioinformatics Bioinformatics applications," *Bioinformatics*, pp. 1–56, 2002.