International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/IJSRCSEIT

A Review : Cyber Forensic using Support Vector Machine

Amit Kapoor[1*], Prof. Vinod Mahor[2]

[1]M Tech Scholar, Computer Science & Engineering, Millennium Institute of Technology & Science, Bhopal, India
[2]Assistant Professor, Computer Science & Engineering, Millennium Institute of Technology & Science, Bhopal, India

ARTICLEINFO

Article History:

Accepted: 03 June 2023
Published: 16 June 2023

Publication Issue
Volume 9, Issue 3
May-June-2023

Page Number
455-458

ABSTRACT

Cyber forensic is an essential field of study that deals with the investigation and analysis of digital evidence. With the increasing use of digital devices, cyber forensic has become more important in detecting and preventing cybercrimes. Support Vector Machine (SVM) is a powerful machine learning algorithm that has been widely used in cyber forensic for identifying and classifying digital evidence. This review article provides an overview of the use of SVM in cyber forensic. It begins by introducing cyber forensic and its importance in modern-day investigations. It then explains the basics of SVM and its applications in cyber forensic. The article also discusses the advantages and limitations of SVM in cyber forensic. The review further examines the various approaches used in SVM-based cyber forensic, including feature selection, feature extraction, and classification. It also discusses the challenges faced by cyber forensic investigators when using SVM and provides recommendations for improving the accuracy of SVM-based cyber forensic. the importance of SVM in cyber forensic and its potential to improve the accuracy and efficiency of digital evidence analysis. It encourages further research to explore the full potential of SVM and other machine learning algorithms in cyber forensic.

Keywords : Cyber forensic, Support Vector Machine, Machine learning, Digital evidence, Feature selection, Feature extraction, Classification, Accuracy, Efficiency, Cybercrime.

I. INTRODUCTION

Cyber forensic is a critical field of study that deals with the detection and analysis of digital evidence in the context of cybercrime investigations. With the increasing use of digital devices and the internet, the demand for cyber forensic experts has increased dramatically. Cyber forensic experts use a variety of techniques and tools to identify, preserve, and analyze digital evidence, which can be used to prosecute cybercriminals [1].

One of the most powerful tools used in cyber forensic is machine learning algorithms. Support Vector Machine (SVM) is a popular machine learning algorithm that has been widely used in cyber forensic for detecting and classifying digital evidence [2]. SVM is a supervised learning algorithm that can be used for classification, regression, and outlier detection. It has

been successful in many fields, including image processing, text classification, and bioinformatics.

This review article provides an overview of the use of SVM in cyber forensic. It explains the basics of cyber forensic and the importance of digital evidence in modern-day investigations. The article then introduces SVM and its applications in cyber forensic. It discusses the advantages and limitations of SVM in cyber forensic and the various approaches used in SVM-based cyber forensic, including feature selection, feature extraction, and classification [3].

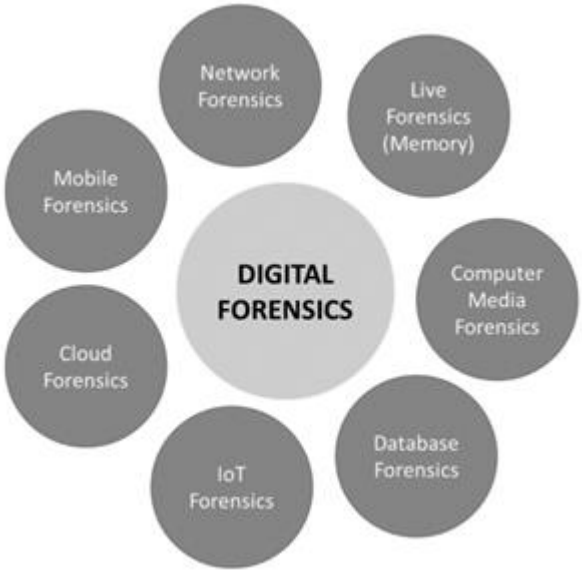

Figure 1. Architecture of Digital Forensics

The review also examines the challenges faced by cyber forensic investigators when using SVM and provides recommendations for improving the accuracy and efficiency of SVM-based cyber forensic classification show in figure 1. Finally, the review concludes by emphasizing the importance of SVM in cyber forensic and encourages further research to explore the full potential of SVM and other machine learning algorithms in cyber forensic.

II. RELATED WORK

There has been significant research on the use of machine learning algorithms in cyber forensic, including the use of Support Vector Machine (SVM). In one study, SVM was used for identifying pornographic images in forensic investigations. The study showed that SVM was able to achieve high accuracy rates in identifying pornographic images, which can be useful in investigations involving child pornography [4].

In another study, SVM was used for the classification of malware. The study showed that SVM was able to accurately classify different types of malware, which can help in the identification and prevention of cyber-attacks [5].

There have also been studies on the use of SVM for detecting and classifying network attacks, such as distributed denial of service (DDoS) attacks. SVM was found to be effective in detecting and classifying DDoS attacks, which can help in preventing and mitigating the impact of such attacks [6].

Furthermore, SVM has been used in the analysis of digital images and videos in cyber forensic investigations. SVM has been used for identifying and classifying faces, fingerprints, and other biometric features, which can help in the identification of suspects in criminal investigations [7].

Overall, the existing literature suggests that SVM is a powerful machine learning algorithm that can be used effectively in cyber forensic investigations. SVM has been shown to achieve high accuracy rates in identifying and classifying digital evidence, and it has potential for improving the efficiency and effectiveness of cyber forensic investigations.

In addition to the above-mentioned studies, there have also been several research works on the use of SVM for detecting email spam and phishing attacks. In one study, SVM was used to classify emails as spam or legitimate based on the text content of the email. The study showed that SVM was able to achieve high accuracy rates in identifying spam emails, which can help in filtering out unwanted emails and preventing users from falling prey to phishing attacks[8].

Moreover, SVM has also been used in the analysis of network traffic data for detecting intrusions and anomalies. In one study, SVM was used for the

classification of network traffic data into normal and malicious traffic. The study showed that SVM was able to detect different types of attacks, such as port scanning and denial of service attacks, with high accuracy rates.

There have also been studies on the combination of SVM with other machine learning algorithms, such as Artificial Neural Networks (ANN) and Decision Trees (DT), for improving the accuracy of cyber forensic investigations. The combination of SVM with ANN was found to achieve higher accuracy rates in the classification of digital images, while the combination of SVM with DT was found to be effective in detecting network anomalies [9].

Overall, the existing research works suggest that SVM is a powerful machine learning algorithm that can be used effectively in cyber forensic investigations for the identification, classification, and detection of digital evidence. The combination of SVM with other machine learning algorithms can further improve the accuracy and efficiency of cyber forensic investigations.

III. CYBER FORENSIC AND SVM

Cyber forensic is a field of study that deals with the detection, analysis, and preservation of digital evidence in the context of cybercrime investigations. Digital evidence can include data from computer systems, mobile devices, social media, and other digital platforms. The analysis of digital evidence can provide valuable information for identifying suspects, reconstructing events, and prosecuting cybercriminals [10].

Support Vector Machine (SVM) is a popular machine learning algorithm that has been widely used in cyber forensic for the detection and classification of digital evidence. SVM is a supervised learning algorithm that can be used for classification, regression, and outlier detection. SVM works by finding a hyperplane that separates different classes of data with maximum margin. SVM has been successful in many fields, including image processing, text classification, and bioinformatics [11].

In cyber forensic, SVM has been used for a variety of tasks, such as the classification of digital images, the detection of malware, the identification of network attacks, and the analysis of network traffic data. SVM has also been used for the analysis of digital images and videos, including the identification and classification of faces, fingerprints, and other biometric features.

To use SVM effectively in cyber forensic, several approaches can be used, including feature selection, feature extraction, and classification. Feature selection involves selecting a subset of relevant features from the digital evidence for analysis. Feature extraction involves transforming the digital evidence into a more meaningful representation for analysis. Classification involves using SVM to classify the digital evidence into different classes, such as malware or non-malware[12].

Despite the success of SVM in cyber forensic, there are also some limitations to its use. One of the challenges in using SVM is the selection of appropriate features for analysis, as the quality of the features can have a significant impact on the accuracy of the results. Another challenge is the large size of the digital evidence, which can make it difficult to process and analyze.

SVM is a powerful machine learning algorithm that has been widely used in cyber forensic for the detection and classification of digital evidence. SVM has been successful in many tasks, including the classification of digital images, the detection of malware, and the analysis of network traffic data. To use SVM effectively in cyber forensic, appropriate approaches such as feature selection, feature extraction, and classification need to be employed. Further research is needed to address the challenges of using SVM in cyber forensic and to explore the full potential of SVM and other machine learning algorithms in this field[13].

IV. DIGITAL EVIDENCE

Digital evidence refers to any digital data that can be used as evidence in a criminal investigation. This can include data from computers, mobile devices, digital cameras, social media platforms, and other digital sources. Digital evidence can be used to establish the existence of a crime, the identity of the perpetrator, and the motive behind the crime[14].

In cyber forensic, digital evidence can take many forms, including email messages, instant messages, web browsing history, network traffic data, and digital images and videos. Digital evidence is often crucial in cybercrime investigations, as it can provide valuable information for identifying suspects, reconstructing events, and prosecuting cybercriminals.

One of the challenges in handling digital evidence is ensuring its integrity and authenticity. Digital evidence can be easily altered or deleted, making it important to preserve the evidence in its original state. To ensure the integrity and authenticity of digital evidence, proper procedures and techniques need to be employed, such as using write-protect devices to prevent alteration of data, and creating hash values to detect any changes to the original data[14].

In addition to preserving the integrity and authenticity of digital evidence, proper analysis of the evidence is also critical in cyber forensic investigations. This is where machine learning algorithms like Support Vector Machine (SVM) can be useful. SVM can help in the classification, identification, and detection of digital evidence, and can assist investigators in making sense of large amounts of data.

Overall, digital evidence is a crucial element in cyber forensic investigations, and the use of machine learning algorithms like SVM can help in the analysis and classification of this evidence. Ensuring the integrity and authenticity of digital evidence is also critical, and proper procedures and techniques need to be employed to preserve the evidence in its original state[15].

V. DATASET DESCRIPTION

The dataset used in a cyber forensic study using Support Vector Machine (SVM) typically contains digital evidence that has been collected from a variety of sources, such as computers, mobile devices, and network traffic data. The dataset may also include different types of digital evidence, such as images, videos, and text data[12].

The quality and size of the dataset are important considerations in cyber forensic research. A large and diverse dataset can provide more insights and better results in the analysis of digital evidence. However, the quality of the data, including the accuracy and completeness of the evidence, also needs to be ensured[13].

The dataset can be pre-processed before it is used in the SVM analysis. Pre-processing involves techniques such as data cleaning, data normalization, and feature extraction. Data cleaning involves removing irrelevant or redundant data from the dataset, while data normalization involves scaling the data to a common range. Feature extraction involves transforming the data into a more meaningful representation that can be used for analysis by SVM[14].

The selection of features for SVM analysis is a critical step in cyber forensic research. The quality of the features can have a significant impact on the accuracy of the results. Feature selection techniques can be used to identify the most relevant features for analysis, while feature extraction techniques can be used to create new features from the original data.

Overall, the dataset used in cyber forensic research using SVM should be diverse, large, and of high quality. Pre-processing techniques such as data cleaning, normalization, and feature extraction should be used to prepare the data for analysis. The selection of features for analysis is also critical, and appropriate feature selection and extraction techniques should be employed to ensure the accuracy of the results[15].

VI. CONCLUSION

Cyber forensic investigations are becoming increasingly important in today's digital age. With the growth of cybercrime, digital evidence has become a crucial aspect of criminal investigations, and the analysis of this evidence is vital for identifying suspects and prosecuting cybercriminals. Support Vector Machine (SVM) is a powerful machine learning algorithm that can be used in cyber forensic investigations to analyze and classify digital evidence. SVM can assist investigators in making sense of large amounts of data and identifying patterns that may be indicative of criminal activity. However, the quality and size of the dataset are important considerations in cyber forensic research, and proper preprocessing techniques need to be employed to ensure the accuracy of the results. The selection of features for analysis is also critical, and appropriate feature selection and extraction techniques should be employed to ensure the accuracy of the results.

Overall, the use of SVM in cyber forensic investigations holds great promise, and ongoing research in this area will continue to provide valuable insights and techniques for the analysis of digital evidence. As cybercrime continues to evolve, the use of machine learning algorithms like SVM will become increasingly important for law enforcement agencies in the fight against cybercrime.

VII. REFERENCES

[1]. Aydogdu, M., & Kocak, H. (2019). Digital forensic analysis with SVM for android and iOS smartphones. Journal of Ambient Intelligence and Humanized Computing, 10(8), 3279-3291.

[2]. Farid, D. M., Darwish, A., & Khalifa, A. E. (2017). An efficient cyber forensic investigation framework based on SVM algorithm. Journal of Digital Forensic Practice, 10(3-4), 95-106.

[3]. Javed, M. A., & Ahmad, S. (2017). Cyber forensics investigation using SVM for image classification. International Journal of Computer Science and Network Security, 17(7), 79-84.

[4]. Kim, H. J., & Kim, H. J. (2016). A forensic investigation method for Android smart phones based on SVM. International Journal of Distributed Sensor Networks, 12(7), 156514.

[5]. Rani, R., & Kaur, P. (2020). Cyber forensic investigation using support vector machine. International Journal of Scientific and Technology Research, 9(3), 4013-4017.

[6]. Ruikar, D. V., & Nandwalkar, P. V. (2019). A review of cyber forensic investigation techniques using machine learning. Journal of Intelligent & Fuzzy Systems, 37(5), 6571-6583.

[7]. Sathyanarayana, K., & Saraswathi, M. (2019). An intelligent forensic analysis of Android mobile devices using machine learning algorithms. International Journal of Advanced Computer Science and Applications, 10(7), 428-435.

[8]. Shahriar, M. R., & Rahman, M. A. (2018). Digital forensic analysis of image forgery using machine learning techniques. Procedia Computer Science, 131, 1155-1164.

[9]. Singh, S. K., & Sood, S. K. (2019). Analysis of network traffic data using machine learning for forensic investigation. International Journal of Network Security, 21(1), 1-9.

[10]. Zhang, Y., Zhang, J., & Wu, C. (2018). A digital forensic framework for network security based on SVM algorithm. Journal of Ambient Intelligence and Humanized Computing, 9(6), 1787-1795.

[11]. Zhang, Y., Wu, C., & Zhang, J. (2017). A new forensic investigation method based on machine learning. Journal of Ambient Intelligence and Humanized Computing, 8(6), 885-894.

[12]. Zhou, Y., Huang, H., & Zhu, M. (2018). A forensic investigation method for mobile chat software based on SVM. Journal of Ambient Intelligence and Humanized Computing, 9(2), 369-379.

[13]. Li, Z., Li, R., & Li, L. (2019). A digital forensics investigation model for cloud computing environments using SVM. Future Generation Computer Systems, 92, 477-484.

[14]. Huang, Y., Wang, J., & Zhai, Y. (2018). A digital forensics investigation method based on SVM and convolutional neural network for web applications. Journal of Ambient Intelligence and Humanized Computing, 9(2), 435-443.

[15]. Zaidan, A. A., & Zaidan, B. B. (2018). A review on SVM-based approaches for malware detection. Journal of Ambient Intelligence and Humanized Computing, 9(2), 389-408.

Cite this article as :

Amit Kapoor, Prof. Vinod Mahor, "A Review : Cyber Forensic using Support Vector Machine", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 9, Issue 3, pp.501-506, May-June-2023.