JOURNAL OF EMERGING COMPUTER TECHNOLOGIES (JECT)

VOLUME: 2 ISSUE NO: 2 YEAR: 2022 PERIOD: JULY-DECEMBER
e-ISSN: 2757-8267

INTERNATIONAL, OPEN ACCESS, PEER-REVIEWED JOURNAL

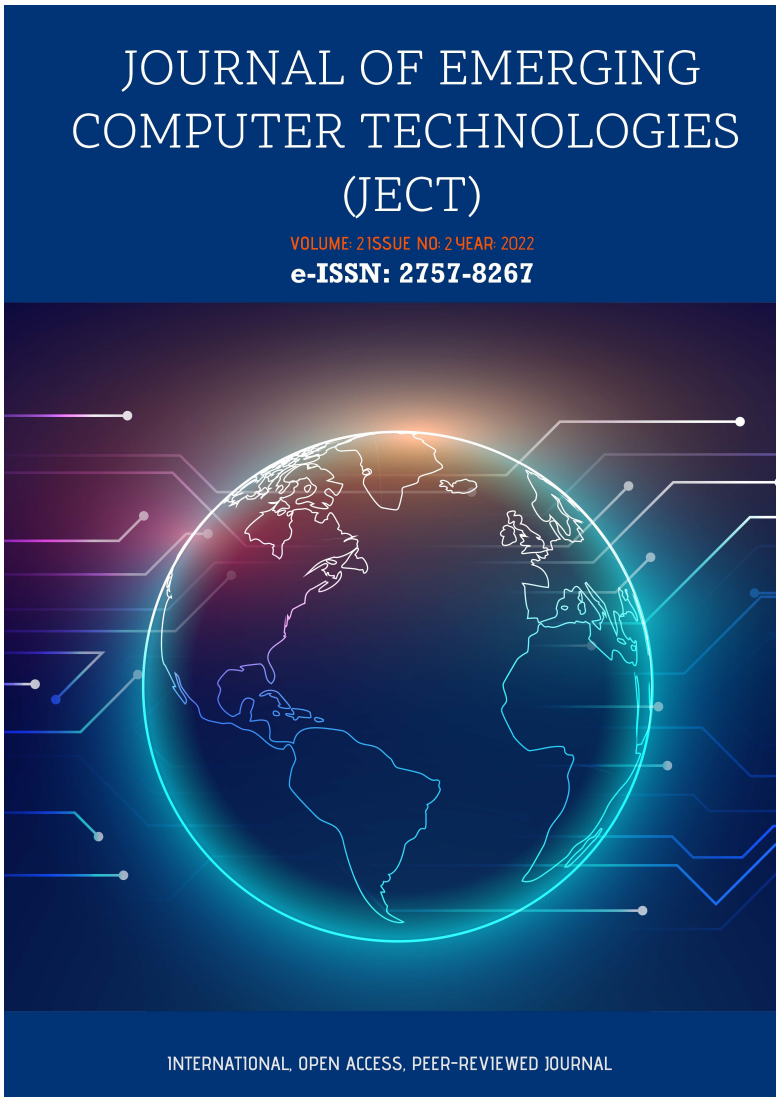
http://dergipark.org.tr/ject

İZMİR AKADEMİ DERNEĞİ

JOURNAL OF EMERGING COMPUTER TECHNOLOGIES (JECT)

E-ISSN: 2757-8267

Volume :2 Number:2 Year:2022



JOURNAL OF EMERGING COMPUTER TECHNOLOGIES (JECT)

is indexed and abstracted by

Index Copernicus

https://journals.indexcopernicus.com/search/details?id=68795

ROAD

https://portal.issn.org/resource/ISSN/2757-8267

Academia.edu

https://gkgkgkg.academia.edu/JournalofEmergingComputerTechnologies

Google Scholar

https://scholar.google.com/citations?user=n986qsIAAAAJ&hl=tr

Asos Index

https://asosindex.com.tr/index.jsp?modul=journal-page&journal-id=2594

Academic Resource Index (Researchbib)

http://journalseeker.researchbib.com/view/issn/2757-8267

OpenAIRE

https://explore.openaire.eu/search/find?fv0=%222757-8267%22&f0=q&active=result

IAD

http://openaccess.izmirakademi.org/index.php/iad/preprints/category/ject

Cosmos

http://www.cosmosimpactfactor.com/page/journals_details/6532.html

EuroPub

https://europub.co.uk/journals/29522

JOURNAL OF EMERGING COMPUTER TECHNOLOGIES

Volume: 2 **No:** 2 **Year:** 2022 **Period:** July-December

Head Office : İzmir
Type of Publication : It is published electronically twice a year, in June and December.
Owner : İzmir Akademi Derneği (İzmir Academy Association)

Journal of Emerging Computer Technologies

Address : Büyükkale Mh. Kerimoğlu Sok. No:40-2 Tire / Izmir, TURKEY
Web : https://dergipark.org.tr/en/pub/ject
Email : journalect@gmail.com
Email : izmirakademidernegi@gmail.com

Journal of Emerging Computer Technologies publishes scientific/original research articles. It is published electronically twice a year, in June and December. It is an **international scientific refereed journal** that publishes articles written in **English**, and includes acedemicians from different countries in its boards. Uses "Double-Blind Peer Review" in reviewing processes. It has adopted the open access principle. No fee is requested from the authors for open access, processing, publication fee or otherwise. It is totally **FREE.**

The responsibility of the articles published in this journal in terms of science and language belongs to the authors. The articles published in the journal cannot be used without reference.

CONTENT

Title / Authors	Type	Pages
Twitter Data Analysis: Izmir Earthquake Case Özgür AĞRALİ Hakan SÖKÜN Enis KARAARSLAN	Research Article	36-41
Measuring The Robustness of AI Models Against Adversarial Attacks: Thyroid Ultrasound Images Case Study Mustafa CEYHAN Enis KARAARSLAN	Research Article	42-47
ASD Automatic Detection by Using Yolo V3 and Yolo V4 Method Farah MUWAFAQ Mesut CEVİK Alzubair ALQARAGHULI	Review Article	48-51
A New Dynamic Supplier Selection and Supplier Evaluation Model in a Company for Decision-Making Process Pınar AZİMLİ Yalçın ÇEBİ	Research Article	52-60
A Review about Forensic Informatics and Tools Çiğdem BAKIR Mecit YUZKAT	Review Article	61-67

Journal of Emerging Computer Technologies
Research Article
Received: *2022-08-07* | ***Reviewing:*** *2022-08-07* & *2022-11-27* | ***Accepted:*** *2022-11-27* | ***Online:*** *2022-11-28* | ***Issue Date:*** *2022-12-31*

Twitter Data Analysis: Izmir Earthquake Case

Özgür AGRALI
Department of Artificial Intelligence
Muğla Sıtkı Koçman University
Muğla, Türkiye
agrali.ozgurr@gmail.com
0000-0001-6974-011X

Hakan SÖKÜN
Department of Artificial Intelligence
Muğla Sıtkı Koçman University
Muğla, Türkiye
hakansokun@posta.mu.edu.tr
0000-0002-0371-8830

Enis KARAARSLAN
Department of Artificial Intelligence
Muğla Sıtkı Koçman University
Muğla, Türkiye
enis.karaarslan@mu.edu.tr
0000-0002-3595-8783

***Abstract*— Türkiye is located on a fault line; earthquakes often occur on a large and small scale. There is a need for effective solutions for gathering current information during disasters. We can use social media to get insight into public opinion. This insight can be used in public relations and disaster management. In this study, Twitter posts on İzmir Earthquake that took place on October 2020 are analyzed. We question if this analysis can be used to make social inferences on time. Data mining and natural language processing (NLP) methods are used for this analysis. NLP is used for sentiment analysis and topic modelling. The latent Dirichlet Allocation (LDA) algorithm is used for topic modelling. We used the Bidirectional Encoder Representations from Transformers (BERT) model working with Transformers architecture for sentiment analysis. It is shown that the users shared their goodwill wishes and aimed to contribute to the initiated aid activities after the earthquake. The users desired to make their voices heard by competent institutions and organizations. The proposed methods work effectively. Future studies are also discussed.**

Keywords: Exploratory Data Analysis, Text Pre-Processing, Disaster Management, Natural Language Processing, Social Media Analysis.

I. INTRODUCTION

An earthquake occurred with its epicenter off the Aegean Sea on October the 30th 2020, around 14:51, and the magnitude of the earthquake was 6.9 [1]. After the earthquake, aftershocks continued in the region. The Izmir earthquake had an impact on many people, both local and in general immediately after it occurred. Great destructions occurred and many people lost their lives. The impact was huge as it is seen in Figure 1.

FIG. 1. AN IMAGE OBTAINED ON THE FIRST DAY OF THE EARTHQUAKE [21]

The public shared their views, especially through social media platforms. Information about people who have relatives in the region or those who may be under the rubble was also shared quite frequently. For this reason, the shares made on Twitter have gained a kind of notification feature. It has also been a guide for those who carry out search and rescue activities.

It is very difficult to directly process and understand the data received from social media platforms that contain different types of data such as Twitter. Social media data is complex and includes a wide variety of data. Making more detailed data analysis on large datasets and using artificial intelligence technologies in decision making for the future can offer effective solutions. The usage can yield effective results. In order to analyze the obtained data correctly, some operations should be applied on the data. These processes are data manipulation, text pre-processing, and feature extraction. In addition, machine learning and artificial intelligence algorithms can be applied depending on the originality of the dataset. In this way, different estimations and analyzes can be performed. In addition, two of the most widely used classification methods in NLP are used: LDA for topic modeling and BERT model for sentiment analysis.

This study includes an exploratory analysis of the posts about the Izmir earthquake. In this context, total of 626,384 tweets were collected. The following operations were performed on these collected tweets: singularization, text preprocessing, feature extraction, sentiment analysis, topic modeling, and visualization. Analyzes were made with the help of these processes.

II. RELATED WORKS

Recently, the processing and analysis of social media data is a topic of great interest. Twitter is one of the most studied social media platforms. E.g; For the analysis of the 2016 US elections [2] and for the air pollution of the 3 big cities of the USA in 2019 [3] Twitter data were studied. In these studies, inferences were obtained by making, machine learning methods and visualizations for analysis.

In this study, about the disasters that occurred in the past years [4], it has been revealed that using the geographical location in the social media posts can be used to identify the people affected by the disaster. In a recent study [5]; It was emphasized that social media sharing during the disaster would be important. In addition, it was stated that aid

organizations and support teams could contribute in the process.

In various studies [6]–[11], sentiment analysis was carried out on social media posts and it was aimed to determine people's attitudes towards events. In the current study in which sentiment analysis was performed in Turkish, classical statistical machine learning methods were used [12]. In another recent study, English sentiment analysis was conducted with the word and rule-based Afinn model, as well as unsupervised learning models such as Textblob and Vader [13]. In these studies, the analysis was carried out with more grouping and classification processes on the posts.

In our study, it is aimed to analyze the data of the posts made during the disaster and to determine the social impact of the inferences obtained from this analysis. It is aimed to reveal the inferences by evaluating the aims, thoughts and starting points of the post owners.

III. Materials and Methods

The methods used in the study are shown in the workflow diagram in Figure 2. General methods in the study; Obtaining Twitter data, pre-processing, analyzing and visualizing. These procedures are explained in the relevant subsection.

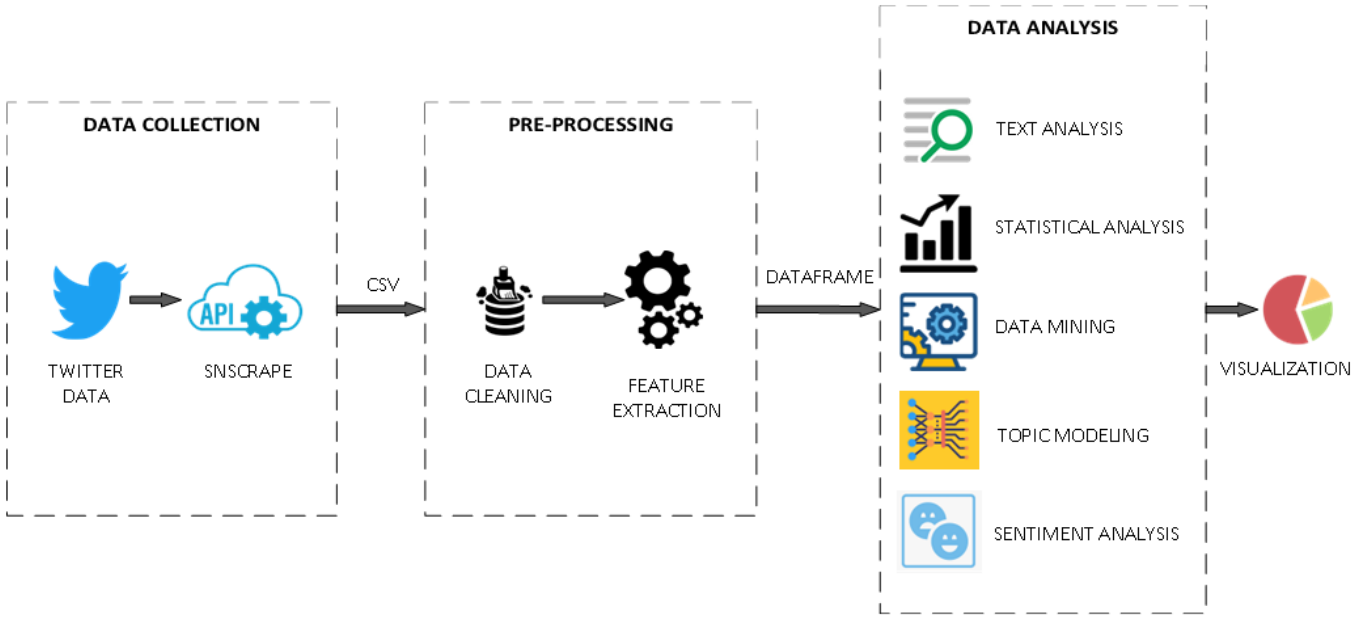


Fig. 2. Data Analysis Flow Diagram

A. Dataset and Extraction of Data

There are many web mining methods available to extract data from Twitter. Many free python libraries are available, such as the Twitter API, twitter-scraper, Twint, snscrape and Selenium tools. There are 5 columns on the Twitter dataset. The columns and their descriptions are shown in Table I. Also features or attributes that can be pulled from Twitter are detailed in Table I.

Table I. Dataset Features

Feature Name	Description	Data Type
Hashtag	With which tag it was taken	String
Datetime	Posted date and time	Datetime
Tweet Id	Unique value identifying	Float
Text	Content of the post	String
Username	Name of the sharing account	String

B. Data Pre-Processing

The data generated by social media users are unstructured data. This data can also be qualified as "dirty data". Users may not follow the rules of the language while sharing, they may have expanded their sharing with emoji, or the text may be corrupted due to a software problem. For these and similar reasons, the texts must go through text pre-processing, which is the first step of exploratory data analysis. The pre-processing steps are listed below.

Step 1- Singularization: It is the deletion of duplicate content. The "Tweet Id" field in the dataset will be checked and deleted.

Step 2- Deletion of Unnecessary Data: It is the removal of unnecessary data and personal data from the dataset. No row loss should occur at the end of this process.

Step 3- Deleting the lost data: There must be text in the "Text" attribute, so this is the process of deleting the records where this field is empty.

Step 4- Formatting the date and time field: The "Datetime" field in the dataset is formatted as "YY-MM-DD HH:mm:ss" in accordance with the analysis.

Step 5- Cleaning/editing the text area: The following corrections are made in the text:

- Deletion of all dirty data types in the share text: link, emoji, special characters,
- Making all characters lowercase,
- Cleaning punctuation marks,
- Removing stop words,
- Deletion of suffixes of words that have suffixes.

C. Feature Extraction

Exploratory data analysis should be done to derive inferences about shared tweets. The most important stage of exploratory data analysis is feature extraction. For this reason, the feature extraction approach is applied. Technically, this stage is also called Feature Engineering. At this stage, new fields are created by grouping, aggregation and statistical operations on the data.

D. Data Analysis

Data analysis is carried out in order to obtain significant results on the collected tweets. In this case, data analysis methods are implemented. First of all, what are the most used words and sentences in the sharing and their semantic evaluation are examined. Then, the information about how often and in what time period the shares are made is examined. Finally, the user accounts that share the most and are tagged the most are compared. In this way, significant inferences based on data will be obtained.

In addition, text analysis should be done to obtain analyzes such as for what purpose the shares are made and which topics are most mentioned. Text analysis is one of the most basic purposes of NLP methods. On the other hand, it will be aimed to obtain inferences from numerical and probabilistic analyzes by examining statistical values. Data mining will be used to explain and make sense of the relationships between text and numerical data. On the other hand, the topic modeling method will be applied to evaluate these shares according to their topic headings. Finally, sentiment analysis will be conducted to show in which emotions these shares are made.

E. Data Visualization

As a result of the analysis, new numerical and text data types are obtained. Different queries are made on these data. Different types of visualizations are made for each data type. It will be aimed to provide earthquake-related determinations by using these visualizations. Another important part is the tags. Tags are the core value in the creation of the dataset. At this stage; Numerical analysis of tags is important.

IV. Implementation

In this study the Python programming language was used and Google Colab was chosen for development. Web mining tool Snscrape and various machine learning software libraries were used.

The shares on Twitter for the Izmir earthquake were examined and it was evaluated that these shares were made through some tags. For this reason, the most used tags were collected manually. These tags are; '#deprem', '#depremizmir', '#enkazaltında', '#egededeprem', '#egedepremi', '#enkaz', '#bayraklı', '#bayraklıdeprem', '#enkazaltinda', '#EnkazIhbarIzmir', '#gecmisolsunizmir', '#izmirdepremi', '#yanındayızimir', '#gecmisolsunizmirim', '#izmirdeprem', '#izmiryanindayiz', '#ˈIzmirDepreminde', '#izmirdepremi', '#izmiryanindayiz', '#izmirgecmisolsun' has been selected.

The data were extracted with the Snscrape library using the specified tag list. The date ranges determined for the collection of data is between October the 30th 2020 and November the 23rd 2020. The day of the earthquake is November the 30th 2020. The date range from which data will be pulled could have been extended further. However, since this study was carried out only on the Izmir earthquake, it was limited to 25 days in order not to deviate from the context.

TABLE II. THE FEATURES OBTAINED AFTER FEATURE EXTRACTION

Feature	Description
Mentioned users list	List of people involved in the share.
List and number of tags	List and number of tags used.
Internet address	Web address list/number in content.
Raw text word count	Word count used in raw text.
Text word count	Post pre-processing word count.
Number of singular words	Number of singular used words.
Number of stop words	Number of stop words used.
Word length	Avg. word length in pre-processed text.
Raw text character count	Number of characters in the raw text.
Number of text characters	Number of characters in the preprocessed text.
Difference in word count	Difference in word count between text

In total, 626,384 tweet lines and 5 feature columns were collected. These data were obtained with 20 different tags that were shared within 24 days after the earthquake occurred. The pre-processing steps described in the method section were applied step by step on the obtained data set. As a result of the operations, the number of data set records is 390,500 and the number of columns is 6. At this point, it is considered that there are repetitive data on the available data set.

Attribute extraction was performed to make inferences about the shares made. The extracted attributes and their descriptions are listed in the Table II. After the feature extraction steps, the number of features in the dataset was 19. The dataset was also run on Orange, which is an open source data mining tool. Table analyzes were performed using more than 2 features.

When it was examined how often the users preferred the tags in the study, it was determined that they mostly used the "#deprem" tag. The hashtag "#deprem", where approximately 250 thousand shares were made, is followed

by ”#izmirdepremi” and ”#izmirdeprem”. It is considered that the posts made mainly focus on these three tags.

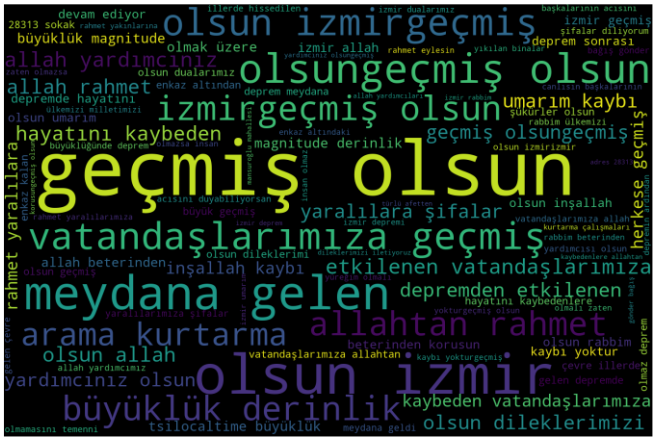


FIG. 3. WORD CLOUD OF THE MOST COMMON BINARY WORDS

For this reason, an analysis was made about which words were used the most in the data set. It has been observed that the most used singular words are “geçmiş”, ”olsun”, “izmir”. The word cloud in the Figure 3 shows the most commonly used binary words. Accordingly, expressions of wish such as “geçmiş olsun” come first. When the triple word groups containing more understandable sentence expressions are examined, the most used triple word group is “geçmiş olsun izmir”. The most used triple word groups, like other word groups, show the atmosphere created by the earthquake.

In this case, it can be thought that the requests and wishes of the users dominate the sharing. After these processes, it is aimed to obtain inferences by making visualizations on the cleaned dataset. In the review of user accounts that shared the most, “TumDepremler” has been the user with more than 2000 shares. The other accounts that share the most are “zelzeleler” and “EMSC”. As a result of the research, it has been understood that these accounts are mostly corporate news sites that give instant earthquake news and accounts that share personal news. It is seen that these users are among the users who tweet the most because they post very frequently and regularly.

In the data set, there are shares starting from the date of the Izmir earthquake on October the 30th 2020, until November the 23rd 2020. 67% of these tweets were posted in October. This reveals that in the first moments of the earthquake, more information flow has been created by users on Twitter.

When the analysis of the month in which the tweets were posted is analyzed, it has been observed that a very high amount of sharing was made between October the 30th and 31st. In the following days, the interest decreased and the number of tweets decreased day by day. As of November the 3rd, it is seen that much fewer posts have been made. In this context, when the dataset is evaluated as a scope, it is concluded that the most shared time is in the first 5 days.

When examining whether a web address is shared or not in the posts about the Izmir earthquake, 51% of the posts do not contain a link, while 45% of them contain 1 web link. This indicates that users did not include any web address in nearly half of the shares.

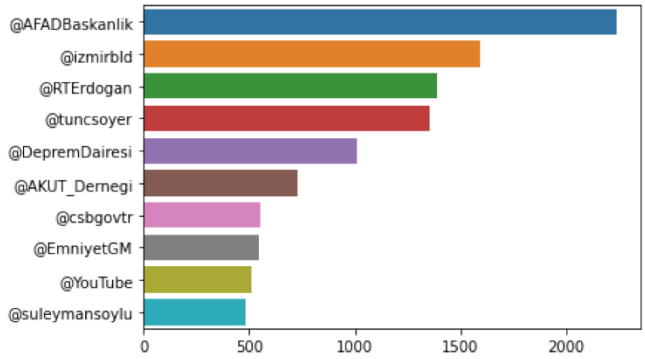


FIG. 4. MOST MENTIONED USERNAMES

In the tweets, the user names mentioned were examined. In this review, it was observed that in most of the shares, users did not tag any users. This explains that users share more to express their feelings.

The most mentioned people in the shared posts are listed in Figure 4. Accordingly, it is seen that users have tagged user accounts that are competent, institutional, and able to contribute to the process, such as ”AFADBaskanlik”, ”izmirbld”, and ”RTErdogan”. When we look at the contents of these posts, it is understood that this was done with the desire to reach the authorities and convey information.

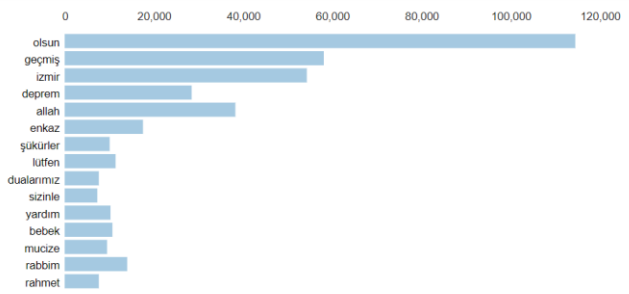


FIG. 5. MOST MENTIONED TOPICS

As it is known, after cleaning tweet texts (removing; stopwords, emojis, punctuation marks, etc.), a smoother text is obtained. To make a more detailed analysis of the shares, these cleaned texts are topic modeling work. Topic Modeling is one of the most used text classification and analysis methods in NLP. In this way, the main theme of the texts is reached in general.

In this study, LDA model was applied to the text contents for the topic modeling analysis. LDA performs word and document analysis using Bayesian theory. It is an unsupervised classification model that tries to predict which word represents which topic in which document by evaluating the words and documents as a whole and separately. The model output made as words and documents

for this study is shown in Figure 5. Accordingly, a classification was made as 15 titles. Although similar results were obtained with the results in the word cloud, it shows that ”yardım” and ”bebek” topics are covered a lot.

Finally, sentiment analysis of the shares was made. Sentiment analysis is a classification problem. As it is known, BERT has achieved great success in the field of NLP, especially for text classification. The Turkish NLP community contributed to the Turkish classification study by developing the BERTurk model. BERTurk is a community-driven BERT model for Turkish.

Two models (pre-trained and fine-tuned) are used in this study. Comparative details of these models are given in Table III.

TABLE III. PRE-TRAINED AND FINE-TUNED MODEL INFORMATION

Model	Class	Epoch	Dataset	Min. Loss	Accuracy
Pre-trained	2	3	48.290	0.16	95%
Fine-tuned	3	3	492.782	0.25	94%

A pre-trained ”bert-base-turkish-sentiment-cased” model was used for BERTurk-based sensitivity analysis [14]. This model is trained with only two classes (negative and positive) data. In this study, a new sentiment analysis classification model that can fine-tune this pre-trained model and make three-class predictions is trained. For the new model obtained, a data set with three class labels (negative, neutral, positive) was used [15]. This dataset contains content where people openly express their feelings, such as Wikipedia and online product reviews. In this case, 90% of this data set is used as training data and 10% as test data in the model. In addition to this, the model trained by Pytorch is set to eval step: 50, learning rate: 5e-7 and batch size: 4. In addition, experiments have observed that hyperparameters affect the success of this model. Accordingly, the fine-tuned model provided a 94% success rate in the test data.

The fine-tuned model had almost the same accuracy as the pre-train with only binary classification. Comparative details of the models are given in Table III. After several trials, it was observed that these values were optimal.

Subsequently, cleaned tweet texts are given as input to this model. It provided dual sentiment classification as positive, neutral and negative as output. It can be seen in Figure 6 that the great majority of these shares are made negative. In addition, it is seen that the most tweeted days are the first five days after the earthquake. On the first day of the earthquake, this 8-floor Rıza Bey apartment, which has more than 40 flats and many workplaces in the Bayraklı district of ˙Izmir, was completely destroyed [16]. For this reason, search and rescue efforts continued for days, especially in this apartment. However, these searches were suspended on November the 1st, 2020. As a result, there was a decrease in the number of tweets posted on November the 1st [17]. In this case, there was a significant increase in the number of positive tweets, equal to the number of negative tweets. This is because 14-year-old İdil was rescued from the wreckage (58 hours after the earthquake) [18].

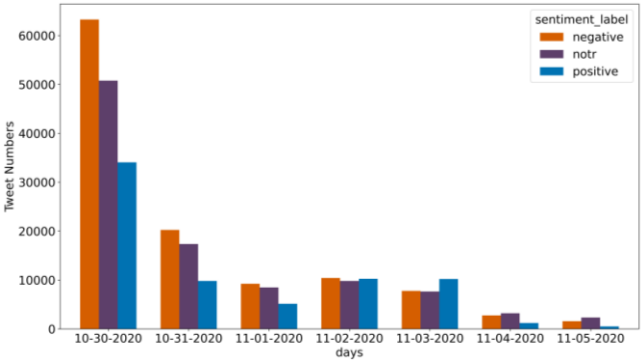


FIG. 6. NUMBER OF TWEETS AND SENTIMENT ANALYSIS FROM DAY TO DAY

On November the 3rd (91 hours after the earthquake), 3-year-old baby Ayda was pulled from the rubble [19]. With this news, there is no decrease in the number of tweets, and it is seen that positive tweets are more than in the first days. For the first time, the number of positive tweets in a day exceeded the number of negative tweets.

Search and rescue efforts ended on November the 4th, 2020 [20], and in the following days, the number of tweets gradually decreased, and the number of negative and neutral tweets increased.

V. DISCUSSION

Most of the posts about the earthquake were made in the first five days. While people conveyed their wishes in the first days, they shared more news and aid issues in the following days. The classification is made based on the topic modelling results. It shows that the people affected by the earthquake wish well, share aid and follow the earthquake news upto-date. The results of the sentiment analysis show that the comments mainly express their sadness about the rescued or harmed people. It is understood that everyone expresses their sadness when bad news is shared during the earthquake, and everyone shares their joy when good news is shared. Without any good or bad developments, neutral content tweets were shared.

The reason why more than half of the shares in the data set do not include any web address is that the vast majority of them are not shared for advertising and news purposes. It is observed that users mostly share using the ”#deprem” tag, and the posts are made especially during lunch hours. The users mainly prefer the most straightforward words to describe the event. Mostly good wishes are made.

The users mainly mention corporate accounts in their posts. Such tweets are analyzed, and it is seen that these institutions are in an effort to contribute to the process and primarily respond to the demands. The most mentioned state officials’ accounts were examined, and it is seen that these institutions share very little when compared to aid

institutions. This situation shows that aid organizations are in two-way communication while state officials are in one-way communication regarding the requests and aid posts on social media.

VI. CONCLUSION

We showed that social media posts could be analyzed to understand the effects of disasters on society and be used to produce solutions. This preliminary study demonstrates the benefits of using artificial intelligence techniques in this process. Similar systems can be deployed to foresee people's feelings and opinions in another possible disaster. Government officials and aid organizations can use these to make instant inferences. They will be able to respond to people's needs more quickly and systematically.

This study is about a current and local event. Creative and practical results have emerged as the applied methods and analyzes are very diverse. It is aimed to get more valuable and multi-class data by conducting more joint studies with social sciences to obtain more comprehensive results in future studies. Comprehensive and specific statistical inferences can be made with these data. Pre-trained BERT models, deep learning, and NLP techniques can be used to perform more than three sentiment classifications and more precise analyses for sentiment analysis.

REFERENCES

[1] A.C Yalciner, et al. "The 30 October 2020 (11: 51 UTC) Izmir-Samos earthquake and tsunami: post-tsunami field survey preliminary results", in Middle East Technical University, Ankara, Turkey, 2020.

[2] A. Bovet, F. Morone and H. A. Makse, "Validation of Twitter opinion trends with national polling aggregates: Hillary Clinton vs Donald Trump", Scientific reports, 2018, 8(1): 1-16.

[3] S. Gurajala, S Dhaniyala., and J. N. Matthews, "Understanding public response to air quality using tweet analysis", Social Media+ Society, 2019, 5(3).

[4] N. Kankanamge, T. Yigitcanlar, A. Goonetilleke and M. Kamruzzaman, "Determining disaster severity through social media analysis: Testing the methodology with South East Queensland Flood tweets", International journal of disaster risk reduction 2020, 42: 101360.

[5] N. Pourebrahim, S. Sultana, J. Edwards, A. Gochanour, and S. Mohanty, "Understanding communication dynamics on Twitter during natural disasters: A case study of Hurricane Sandy", International journal of disaster risk reduction, 2019, 37: 101176.

[6] A. Ceron, L. Curini, S.M. Iacus and G. Porro, "Every tweet counts? How sentiment analysis of social media can improve our knowledge of citizens", political preferences with an application to Italy and France. New media and society, 2014, 16(2): 340-358.

[7] V. Kharde and P. Sonawane, "Sentiment analysis of twitter data: a survey of techniques", arXiv preprint arXiv:1601.06971, 2016.

[8] A. Shelar, C.Y. Huang, "Sentiment analysis of twitter data", In: 2018 International Conference on Computational Science and Computational Intelligence (CSCI). IEEE, 2018. p. 1301-1302.

[9] M. Albayrak, K.topal and V. Altıntaş, "Sosyal medya üzerinde veri analizi: Twitter", Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, 2017, 22(Kayfor 15 Özel Sayısı): 1991-1998.

[10] A. Karami, V. Shah, R. Vaezi and A. Bansal, "Twitter speaks: A case of national disaster situational awareness", Journal of Information Science, 2020, 46(3): 313-324.

[11] K. Zahra, M. Imran, and F. O. Ostermann, "Automatic identification of eyewitness messages on twitter during disasters", Information processing management, 2020, 57(1): 102107.

[12] F. Dalkılıç, , A. Çam, "Automatic Movie Rating by Using Twitter Sentiment Analysis and Monitoring Tool", Journal of Emerging Computer Technologies, 2021, 1(2): 55-60.

[13] Ö. Ağralı, Ö. Aydın, "Tweet Classification and Sentiment Analysis on Metaverse Related Messages", Journal of Metaverse, 2021, 1(1): 25-30.

[14] S. Yıldırım, savasy/bert-base-turkish-sentiment-cased · Hugging Face, 2020. [Online]. Available: https://huggingface.co/savasy/bert-baseturkish-sentiment-cased. [Accessed: 02- Nov- 2020].

[15] B. Ayhan, winvoker/turkish-sentiment-analysisdataset Hugging Face, 2022. [Online]. Available: https://huggingface.co/datasets/winvoker/turkish-sentiment-analysisdataset. [Accessed: Nov- 2022].

[16] "İşte birçok kişiye mezar olan Rıza Bey apartmanı", 2020. [Online]. Available: https://www.turkiyegazetesi.com.tr/gundem/742966.aspx. [Accessed: Oct. 30, 2020].

[17] T. Albay, "İzmir'de deprem sonrası yıkılan Rıza Bey Apartmanı enkazındaki kurtarma çalışmasına ara verildi", 2020. [Online]. Available: https://www.aa.com.tr/tr/turkiye/izmirde-deprem-sonrasi-yikilan-rizabey-apartmani-enkazindaki-kurtarma-calismasina-ara-verildi-/2027207. [Accessed: 01- Nov- 2020].

[18] T. Albay, "İzmir'deki depremden yaklaşık 58 saat sonra 14 yaşındaki İdil enkazdan yaralı çıkarıldı", 2020. [Online]. Available: https://www.aa.com.tr/tr/turkiye/izmirdeki-depremden-yaklasik-58-saatsonra-14-yasindaki-idil-enkazdan-yarali-cikarildi/2027463. [Accessed: 02- Nov- 2020].

[19] "Son dakika: 3 yaşındaki Ayda bebek 91'inci saatte enkazdan çıkarıldı", 2020. [Online]. Available: https://www.haberturk.com/son-dakikahaberi-tunc-soyer-acikladi-ekipleri-bir-bebege-canli-ulasti-2857124. [Accessed: 03-Nov-2020].

[20] "İzmir depremi: Arama kurtarma çalışmaları sona erdi, can kaybı 114'e yükseldi", 2020. [Online]. Available: https://www.bbc.com/turkce/haberler-turkiye-54810440. [Accessed:04- Nov- 2020].

[21] L. İlhan "İzmir'de deprem", 2020. [Online]. Available: https://www.aa.com.tr/tr/pg/foto-galeri/izmir-de-deprem/0. [Accessed: 30- Oct- 2020].

Journal of Emerging Computer Technologies
Research Article
Received: *2022-10-25* | ***Reviewing:*** *2022-11-08 & 2022-12-13* | ***Accepted:*** *2022-12-13* | ***Online:*** *2022-12-14* | ***Issue Date:*** *2022-12-31*

Measuring The Robustness of AI Models Against Adversarial Attacks: Thyroid Ultrasound Images Case Study

Mustafa Ceyhan
Huawei Turkey R&D Center / Artificial Intelligence MsC, Mugla Sitki Kocman University
Istanbul, Türkiye
0000-0003-3268-6898
mustafac94@gmail.com

Enis Karaarslan
Department of Computer Engineering
Mugla Sitki Kocman University
Mugla, Türkiye
0000-0002-3595-8783
enis.karaarslan@mu.edu.tr

***Abstract*— The healthcare industry is looking for ways on using artificial intelligence effectively. Decision support systems use AI (Artificial Intelligence) models that diagnose cancer from radiology images. These models in such implementations are not perfect, and the attackers can use techniques to make the models give wrong predictions. It is necessary to measure the robustness of these models after an adversarial attack. The studies in the literature focus on models trained with images obtained from different regions (lung x-ray and skin dermoscopy images) and shooting techniques. This study focuses on thyroid ultrasound images as a use case. We trained these images with VGG19, Xception, ResNet50V2, and EfficientNetB2 CNN models. The aim is to make these models make false predictions. We used FGSM, BIM, and PGD techniques to generate adversarial images. The attack resulted in misprediction with 99%. Future work will focus on making these models more robust with adversarial training.**

Keywords*— *Adversarial Attack, CNN Models, Thyroid Ultrasound Images, Machine Learning, Deep Learning

I. INTRODUCTION

Today, applications of artificial intelligence such as object detection, voice recognition, recommendation systems, credit risk estimations, and disease diagnosis are widely used in many sectors such as health, finance, robotics, agriculture, marketing, and education. AI is increasingly used in the healthcare industry, especially in radiology (1). Applications developed using artificial intelligence in cancer diagnosis allow radiologists to make faster and more reliable diagnoses. Several models are used for different diseases and cancer types of the brain (2), skin (3), breast (4), lung (3) and thyroid (5) using different types of medical images. Models trained with these images usually have successful results. Researchers continue to try new techniques with new data and new models.

Artificial intelligence is a black box application that can predict a situation by learning from structured or unstructured data. In cases where mathematics and statistics cannot conclude, they can catch patterns in the data and reach the correct result with high accuracy rates. Classical machine learning algorithms have been used successfully and continue to be used for a long time. However, classical machine learning algorithms cannot achieve the desired success in some areas like image recognition or natural language processing. We can use deep learning to overcome this problem. Learning has become better by adding multiple hidden layers to artificial neural networks. We can achieve deeper learning with this method and capture the patterns between the inputs better. CNN models, which are different versions of neural networks, are used for image recognition and classification, but these models are open to adversarial attacks. The attackers can use several attack methods to fool artificial intelligence models. These can cause the models to give false results. This can have unacceptable outcomes in the healthcare industry.

In this study, we applied attack techniques to evaluate thyroid ultrasound images. This data type was chosen as the literature lacked using attack techniques against a model trained with thyroid ultrasound images. We are using a two-output model developed for the diagnosis of thyroid cancer. This model returns whether the patient has cancer based on the input image. In this study, we tested VGG19, Xception, ResNet50V2, and EfficientNetB2 CNN models against the adversarial images generated using FGSM, BIM, and PGD techniques on an ultrasound image dataset. The major contribution of this paper is to show that artificial intelligence models trained for thyroid diagnosis using thyroid ultrasound images have a vulnerability to adversarial images.

We give a literature survey and present a brief background on Convolutional Neural Networks models for medical diagnosis and Adversarial Attacks to these models in section 2. In section 3, the method is given. The implementation is presented in section 4. The discussion is given in section 5. Finally, we conclude in section 6 with a hint of future works.

II. FUNDAMENTALS

A. Literature Survey

Finlayson et. al trained three models with three different datasets in their study (3). These are fundoscopy images for diabetes disease, x-ray images for pneumothorax disease, and dermoscopy images for skin cancer. They have performed successful white-box PGD attacks on the trained models. Bortsova et al. conducted black box attacks on diabetes, pneumothorax, and pathology data and achieved successful results (6). Alexandra et al. used FGSM, and JSMA techniques on a model developed for brain and lung cancer diagnosis and achieved successful results (7).

Goodfellow et al. demonstrated that artificial intelligence models can be fooled by perturbing the input image with noise calculated by the FGSM algorithm (8). This

Cite (APA): Ceyhan, M., Karaarslan, E. (2022). Measuring The Robustness of AI Models Against Adversarial Attacks: Thyroid Ultrasound Images Case Study. *Journal of Emerging Computer Technologies*, 2(2), 42-47.
Volume:2, ***No***:2, ***Year:*** 2022, ***Pages:*** 42-47, December 2022, *Journal of Emerging Computer Technologies*

attack tries to calculate the noise in the direction of the gradient, which will increase the loss of the model in one step. After calculating the gradient, the minimum amount is added to the input image that makes the model cross the decision boundary. This amount of addition is adjusted with epsilon. In another study published in 2017 by Goodfellow et al., they introduced the BIM algorithm, which is the iterative version of the FGSM attack (9). This algorithm calculates minimum perturbation more effectively using multiple steps. At each step, the algorithm tries to find the minimum perturbation by gradually increasing the epsilon value. Madry et al. used the PGD method similar to the BIM algorithm in 2017 (10). Different algorithms in the literature will perturb the input data to make it wrongly guessed. Among them, Jacobian-based Saliency Map Attack (11), DeepFool (12), Carlini & Wagner Attack (13), One Pixel Attack (14), and Adversarial Patch (15) are the leading effective attack techniques. Most of these studies have been tried on Image-Net (16), MNIST (17), and CIFAR (18) datasets and have shown successful results.

B. Convolutional Neural Networks

Convolutional neural network (CNN) is the most well-established method among the numerous deep learning models (19). CNN can be applied to different fields such as image classification, object detection, time series, and natural language processing. In simple terms, the properties of the input data are extracted in the convolutional and pooling layers. These extracted features are turned into a vector, and the weights of the deep neural network are trained. The most important part here is the feature extraction part. The better the feature extraction part, the more accurately the parameters of dense layers can be calculated. Various techniques have been developed since the first feature extraction applications such as LeNet and AlexNet, VGG19, Resnet50V2, Xception, and EfficientNetB2 are the most widely used models.

VGG19 (20) is a classic CNN model. Since the LeNet model, more convolution and pooling layers have always been added to the feature extraction part to achieve better results. VGG19 is a continuation of this tradition and consists of 16 convolution and 5 pooling layers in total. It has too many parameters and a high volume because the parameter feature mitigation layer is not applied.

ResNet (21) architecture is a model developed as an alternative to traditional feature extraction architecture. Adding more convolution and pooling layers does not increase the accuracy values after a certain level. Adding more of these layers causes the gradient to vanish or explode after a while. A strategy called residual nets has been developed to prevent this and to get more efficient results in fewer layers.

Xception (22), is a model based on the Inception model. It uses an approach called depthwise separable convolutions. It consists of blocks that try to capture different features with different filters. The model is formed from the combination of these blocks.

EfficientNet (23), one of the most recently developed models, and its derivatives can be considered the best in its field now. EfficientNet model versions are among the most successful feature extraction algorithms. It scales the model in depth, width, and resolution to get a better model.

C. Adversarial Attacks

Adversarial attacks are attempts to fool artificial intelligence models. Barreno et al. listed these attacks and their types comprehensively for the first time in their study "Can Machine Learning be Secure" (24). Artificial intelligence security is discussed more comprehensively in the study called “The Security of Machine Learning” (25). Attacks can be classified into different sub-categories such as the attacker's impact, knowledge, and specificity (26).

*1) Attacks based on the influence of the attacker :*These attacks are: causative attacks, evasion attacks and exploratory attacks.

Causative attacks occur in the training part of the model. These attacks are also called poisoning attacks. Data is added to the dataset, which will cause the model parameters to be miscalculated during training. Data poisoning can be the swapping of labels of training data or specially crafted data. It is used in attacks against models that are constantly trained with new data coming from outside in real-world scenarios.

Evasion attacks are performed on a trained model. The attacker makes an attempt to fool the model with perturbed data, that is, with adversarial examples. The attack occurs by adding noise to the data. Incorrect predictions are targeted by adding various noises. However, the important point here is that adversarial examples cannot be noticed by the human eye. Gradient-based adversarial example generation algorithms are the most successful noise addition methods. The study of Goodfellow et al. (8) can be considered a pioneer in applying this attack to images. Adversarial examples can be formed quickly and cheaply with their FGSM algorithm.

Exploratory attacks are based on a trained model such as evasion. The purpose here is to gather information about the model. It can be used to launch another attack in the future based on the gathered information.

2) Attacks based on the attacker knowledge: These attacks are white box and black box attacks. In white box attacks, the attacker knows the model and its parameters. In black box attacks, the attacker does not know the model and parameters.

3) Attacks based on attacker specificity: These attacks are targeted and untargeted. In targeted attacks, the perturbed data is asked to correctly predict a selected class instead of the actual class. In untargeted attacks, the aim is simply to misclassify the model.

III. METHOD

Thyroid ultrasound images were used as a dataset. These images are inherently noisy data (27). Therefore, more complex and deep models are more successful for feature extraction. Convolutional neural networks are used to train the data. Then Adversarial attack algorithms are used to attack the model.

A. Dataset

We used a dataset of Thyroid Ultrasound images like Fig 1 from Kaggle for the training application (29). There are 3282 cancer-free images and 4006 cancer-containing images in the dataset. The dataset is formed of training, testing, and validation sections. These sections are preprocessed for each model for training.

B. Preprocessinn and Training

Convolutional Neural Networks (CNN) are used in this study. CNN model is used in different architectures for training. Four different models (VGG19, Resnet50V2, Xception, and EfficientNetB2) are used. The characteristics of the models are given in Table 1. EfficientNetB2 expects each input pixel to be in the normal value range of 0-255 (23). Other models scale from 0-1 (20-22). Data is fitted to each model during this preprocessing.

TABLE I. THE FEATURES OF THE MODELS

Model	**Size (MB)**	**Top-1 Acc.**	**Top-5 Acc.**	**Param.**	**Depth**
VGG 19	549	71.3%	90%	90M	19
ResNet50V2	98	76%	93%	93M	103
Xception	88	79%	94.5%	94.5M	81
EfficientNetB2	36	80.1%	94.9%	94.9M	186

C. Attack Algorithms

Three different attack algorithms were used for the attack. These are respectively FGSM, BIM, and PGD algorithms. The purpose of these attack algorithms is to perturb the input image. But the important thing here is that the perturbed image cannot be distinguished by the human eye. False estimates can also be given by adding noises like Gaussian noise (28), but the human eye can detect these images. Gradient-based algorithms are the most suitable algorithms for calculating minimum noise.

The working principle is briefly as follows. During the training phase, many images are given to the model. A loss is calculated for each input. In backpropagation, the weights of the model are optimized with this calculated loss. The aim is to reduce the loss value of the model to the minimum value. Optimization is done with the gradient of the loss function. We try to reach the slope of the loss function close to zero. The aim is to maximize the loss function in the attack algorithms. For this, the gradient value is taken for each image pixel, and the mark function is used. Gradient values are the direction vector that shows how close they are to the correct class. A certain amount of these gradient values is added to the input image so that it crosses the correct class boundary.

In the FGSM algorithm (1) shown in Equation (1), the amount of perturbation is found in one step. The signed gradient is multiplied by a certain epsilon value and added to the input image. It is an untargeted attack. The goal is to make another class guess.

$$X^{adv} = X + \epsilon sign(\nabla_X J(\theta, X, y)) \quad (1)$$

X is the image sent to the model for prediction. y is the correct label of the image. J is the loss function that calculates the loss of the input. ∇ calculates the gradients of the input according to the loss function. Gradients extracted with the Sign function are signed. The values obtained with the sign function are added to the input image by a certain amount of ϵ. Even if the image seems unchanged when viewed with the human eye, the image has changed mathematically. When the model is asked to predict with the adversarial example produced by the added noise, it maximizes the loss function, and the model predicts the input incorrectly.

In the BIM algorithm shown in Equation (2), the amount of perturbation is found by increasing the epsilon value in each iteration. It is slower than FGSM, but more stable adversarial images can be obtained.

$$X_0^{adv} = X,\ X_0^{adv} = Clipx,\epsilon\{X_N^{adv} + \alpha sign(\nabla_X J(\theta, X_N^{adv}, y))\} \quad (2)$$

The PGD algorithm is the iterative version of the FGSM algorithm. It is a different version of the BIM algorithm. Unlike BIM, it uses random values at each iteration to find the best perturbation.

IV. IMPLEMENTATION

The implementation steps are as in Fig 2 and each step is explained one by one.

TABLE II. TRAINING PARAMETERS

Training Parameters	**Selected Parameters**
Loss Function:	Categorical Cross-Entropy
Optimizer:	Adamax
Learning Rate:	0.001
Batch-size:	30

We selected four different CNN models for model training. The selected models were VGG19, ResNet50V2, Xception, and EfficientNetB2, respectively. Keras library is used. We used transfer learning with models whose weights were pre-trained with image-net. We fine-tuned the dense layer according to the new model. The output layer is set to its new two classes. The model is trained with new data. Training parameters are as in the Table 2.

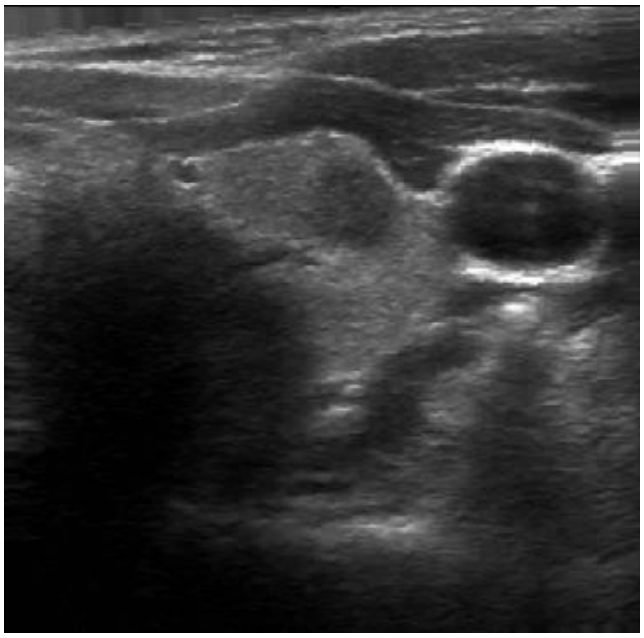


FIG 1. THYROID ULTRASOUND IMAGE

As a result of the training, the test accuracy values were 0.93 for EfficientNetB2, 0.89 for Xception, 0.83 for Resnet50v2, and 0.72 for VGG19. The EfficientNetB2 model with the highest depth achieved the best accuracy. The Xception and ResNet50V2 model have similar parameter numbers and depth values. Although ResNet50V2 is slightly deeper than the Xception model in depth, it did not give a better result. This may be due to different model architectures. ResNetV2 uses deep residual networks and Xception uses depth-wise separable convolutions. VGG19 is the oldest model of all. It has traditional architecture and a large number of parameters. It is also heavy in size, but it is a shallow model. Therefore, we cannot say that it is very successful in complex images.

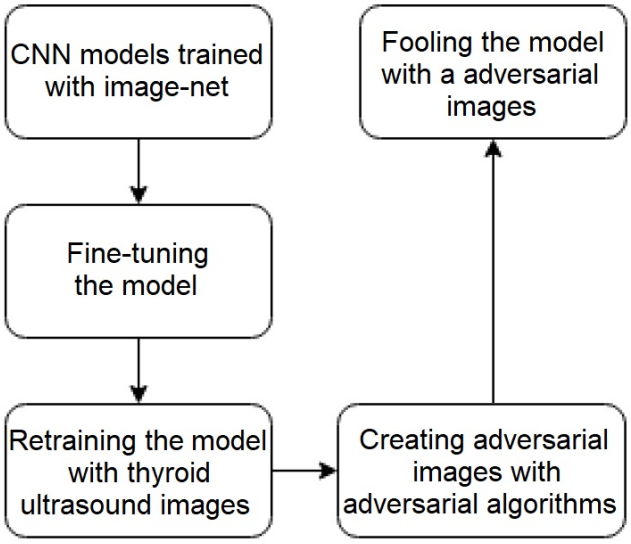


FIG 2. IMPLEMENTATION STEPS

We used the IBM Adversarial Robustness Toolbox library for implementing attacks (30). White-box targeted and white-box untargeted evasion attacks were performed on the trained models. These attacks are FGSM, BIM, and PGD attacks, respectively. The FGSM white box is an untargeted attack. BIM and PGD are white-box targeted attacks. The results are shown in Figs 3-6 and Table 3 and discussed in the next section.

V. RESULT AND DISCUSSION

In the graphs shown in Fig 3-4-5, each line represents the prediction accuracy of a model at different epsilon values. The positive part of the y-axis of the graph indicates that the model is classifying correctly. The corresponding values are the accuracy rate. The negative part of the y-axis of the graph is the false class prediction accuracy of the model deceived by the Adversarial image.

The incorrect prediction accuracy rates of the models at different epsilon values with the FGSM technique are shown in Fig 3. Applying the FGSM attack to EfficientNetB2, Xception, and ResNet50V2 models added 0.01 epsilon-generated noise to the input image. The adversarial images created with the added noise caused the models to predict incorrectly with an accuracy of 99%. Epsilon 0.01 was sufficient for BIM and PGD iterative attacks against these models.

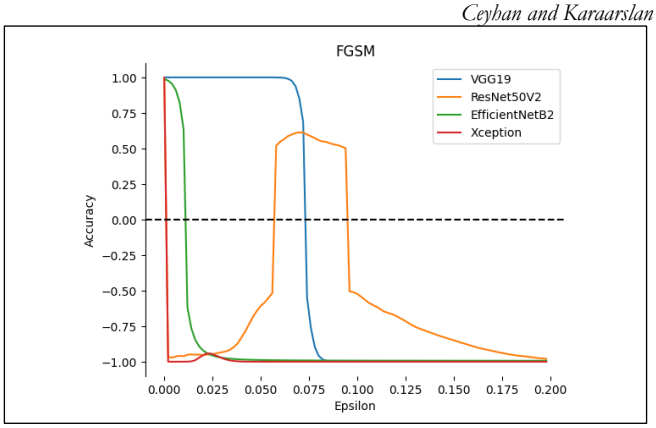


FIG 3. MISCLASSIFICATION ACCURACY RATES OF 100 DIFFERENT EPSILON VALUES BETWEEN 0-0.2 ON FOUR DIFFERENT CNN MODELS USING THE FGSM TECHNIQUE.

As can be seen in Fig. 3, different outputs were obtained in the ResNet50V2 model as a result of the perturbation made by the FGSM technique. The model predicted incorrectly with the epsilon values mentioned earlier and passed the decision boundary. However, we saw that it again came to the correct prediction region in some intervals. The model, which made an incorrect prediction at epsilon values between 0.04 and 0.06, started to make an accurate prediction between 0.06 and 0.08 epsilon values again. It continued to predict incorrectly at 0.08 and higher values. Images were perturbed with epsilon values between 0 and 16 to examine whether models at higher epsilon values obtained a similar result.

As shown in Fig 4, the situation seen for ResNet50V2 was also seen for EfficientNetB2 in the examination with epsilon values of 0-16. In Xception and VGG19, it was observed that the accuracy of false predictions increased in direct proportion to the increase in epsilon.

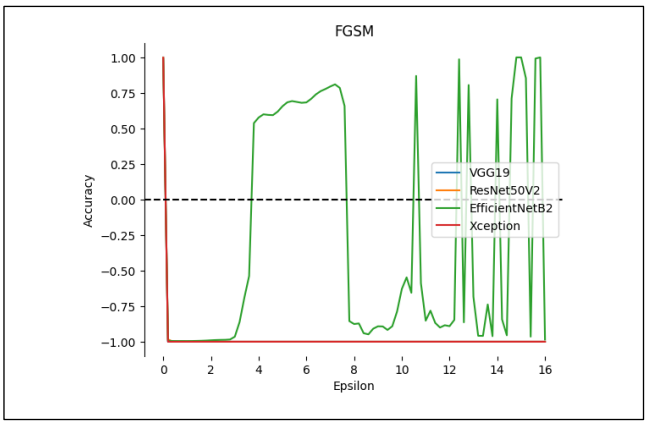


FIG 4. MISCLASSIFICATION ACCURACY RATES OF 100 DIFFERENT EPSILON VALUES BETWEEN 0-16 ON FOUR DIFFERENT CNN MODELS USING THE FGSM TECHNIQUE. (THE BLUE AND ORANGE LINES ARE BELOW THE RED LINE, AS THEY HAVE SIMILAR VALUES.)

As seen in Fig 5, these deviations in FGSM do not exist in BIM and PGD, which are the iterative methods of obtaining adversarial images. The accuracy rate of incorrect estimation increased with the increase in the epsilon value of iterative methods. This experiment proves that iterative methods are more powerful and stable techniques.

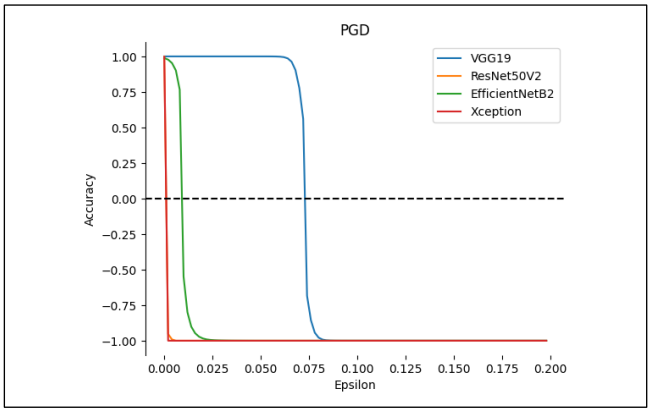


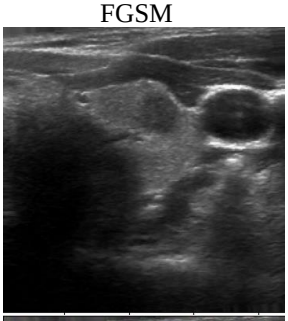
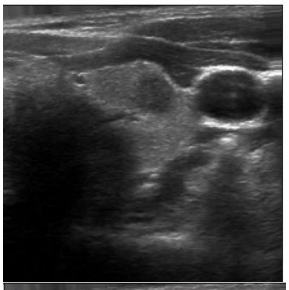
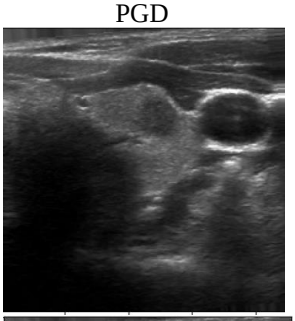
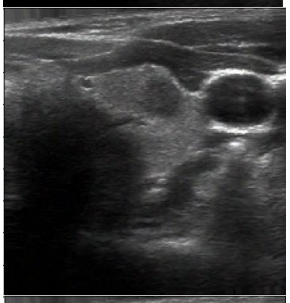
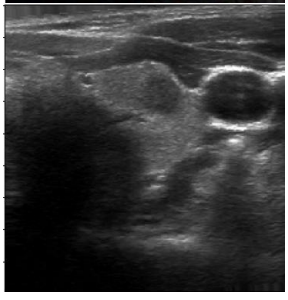
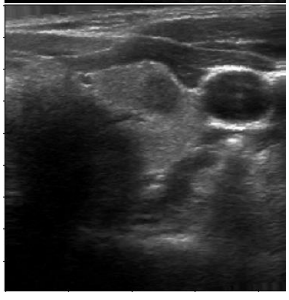
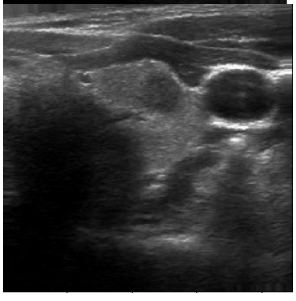
FIG 5. MISCLASSIFICATION ACCURACY RATES OF 100 DIFFERENT EPSILON VALUES BETWEEN 0-0.2 ON FOUR DIFFERENT CNN MODELS USING THE PGD TECHNIQUE. (THE ORANGE LINE IS BELOW THE RED LINE, AS THEY HAVE SIMILAR VALUES.)

Another interesting result is that the VGG19 model, which has the highest number of parameters but the lowest depth, is more difficult to fool than other models. EfficientNetB2 was the second strongest model, which was hard to fool. Xception and ResNet50V2 were the most easily fooled models. These may have different causes, such as depth and model architecture. As depth increases and model architectures change, it can cause blind spots on models to increase.

The images mostly gave good results with different epsilon values. There can always be exceptions. Some of the images can fool different models with different amounts of perturbation.

The creation process of adversarial images is shown in Fig 6, and all the hostile images generated are shown in Table 3. The original image in the table has thyroid disease. When the prediction is made with trained models, cancer can be detected. After adding noise with attack algorithms, %99 percent of non-cancerous prediction was provided. The remarkable point is that the added noises cannot be distinguished by the human eye.

TABLE III. ADVERSARIAL IMAGES PRODUCED WITH DIFFERENT MODELS AND ATTACK ALGORITHMS

	FGSM	BIM	PGD
VGG19			
RESNET50V2			
XCEPTİON			
EFFİCİENTNETB2			

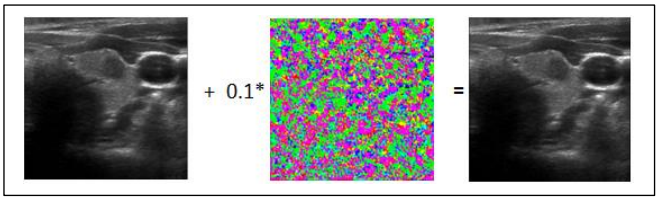


FIG 6. ADVERSARIAL IMAGE GENERATION FROM THE EFFICIENTNETB2 MODEL WITH THE FGSM ALGORITHM. (FORMULA 1)

VI. CONCLUSION

In the study, we tried attack algorithms on thyroid ultrasound images on the widely used models. The models incorrectly predicted with early every perturbed image. Artificial intelligence models trained from thyroid ultrasound images are successfully fooled. The possibility of cheating each model with different amounts of perturbation values is shown. These weaknesses form a problem that needs to be fixed. Artificial intelligence models developed for diagnosis need to be made stronger against attacks. In the continuation of the study, we aim to work on more robust models against these attacks with adversarial learning.

REFERENCES

[1] A. Hosny, C.Parmar, J.Quackenbush, L. H. Schwartz, and H. J. W. L. Aerts "Artificial intelligence in radiology." *Nature Reviews Cancer*, Aug., pp. 500-510, 2018

[2] G. S. Tandel, M. Biswas, O. G. Kakde, A. Tiwari, H. S. Suri, M. Turk et al., "A review on a deep learning perspective in brain cancer classification," *Cancers*, vol. 11, no. 1, p. 111, 2019.

[3] S. G. Finlayson, J. D. Bowers, J. Ito, J. L. Zittrain, A. L. Beam, and I. S. Kohane, "Adversarial attacks on medical machine learning," *Science*, vol. 363, no. 6433, pp. 1287–1289, 2019.

[4] B. Ehteshami Bejnordi, M. Veta, P. Johannes van Diest, B. van Ginneken, N. Karssemeijer, G. Litjens et al. "Diagnostic assessment of deep learning algorithms for detection of lymph node metastases in women with breast cancer," *JAMA*, vol. 318, no. 22, p. 2199, 2017.

[5] F. Abdolali, A. Shahroudnejad, S. Amiri, A. Rakkunedeth Hareendranathan, J. L. Jaremko et al. "A systematic review on the role of artificial intelligence in sonographic diagnosis of thyroid cancer: Past, present and future," *Frontiers in Biomedical Technologies*, 2021.

[6] G. Bortsova, C. González-Gonzalo, S. C. Wetstein, F. Dubost, I. Katramados, L. Hogeweg et al. "Adversarial attack vulnerability of medical image analysis systems: Unexplored factors," *Medical Image Analysis*, vol. 73, p. 102141, 2021.

[7] A. Vatian, N. Gusarova, N. Dobrenko, S. Dudorov, N. Nigmatullin, A. Shalyto et al. "Impact of adversarial examples on the efficiency of interpretation and use of information from high-tech medical images," *2019 24th Conference of Open Innovations Association (FRUCT)*, 2019.

[8] I. J. Goodfellow, J. Shlens, and C. Szegedy, "Explaining and Harnessing Adversarial Examples." 2014 [Online]. Available: http://arxiv.org/abs/1412.6572

[9] A. Kurakin, I. Goodfellow, and S. Bengio, "Adversarial examples in the physical world." 2016 [Online]. Available: http://arxiv.org/abs/1607.02533

[10] A. Madry, A. Makelov, L. Schmidt, D. Tsipras, and A. Vladu, "Towards Deep Learning Models Resistant to Adversarial Attacks," 2017 [Online]. Available: http://arxiv.org/abs/1706.06083

[11] N. Papernot, P. McDaniel, S. Jha, M. Fredrikson, Z. B. Celik, and A. Swami, "The limitations of deep learning in adversarial settings," *2016 IEEE European Symposium on Security and Privacy (EuroS&P)*, 2016.

[12] S.-M. Moosavi-Dezfooli, A. Fawzi, and P. Frossard, "DeepFool: A simple and accurate method to fool Deep Neural Networks," *2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 2016.

[13] N. Carlini and D. Wagner, "Towards evaluating the robustness of neural networks," *2017 IEEE Symposium on Security and Privacy (SP)*, 2017.

[14] J. Su, D. V. Vargas, and S. Kouichi, "One pixel attack for fooling deep neural networks." 2017 [Online]. Available: http://arxiv.org/abs/1710.08864

[15] T. B. Brown, D. Mané, A. Roy, M. Abadi, and J. Gilmer, "Adversarial Patch," 2017 [Online]. Available: http://arxiv.org/abs/1712.09665

[16] J. Deng, W. Dong, R. Socher, L. -J. Li, Kai Li and Li Fei-Fei, "ImageNet: A large-scale hierarchical image database," *2009 IEEE Conference on Computer Vision and Pattern Recognition*, 2009, pp. 248-255, doi: 10.1109/CVPR.2009.5206848.

[17] D. C. Ciresan, U. Meier, J. Masci, L. M. Gambardella, and J. Schmidhuber, "High-Performance Neural Networks for Visual Object Classification," *CoRR*, vol. abs/1102.0183, 2011 [Online]. Available: http://dblp.uni-trier.de/db/journals/corr/corr1102.html#abs-1102-0183

[18] A. Krizhevsky, "Learning Multiple Layers of Features from Tiny Images," pp. 32--33, 2009 [Online]. Available: https://www.cs.toronto.edu/~kriz/learning-features-2009-TR.pdf

[19] S. Albawi, T. A. Mohammed and S. Al-Zawi, "Understanding of a convolutional neural network," *2017 International Conference on Engineering and Technology (ICET)*, 2017, pp. 1-6, doi: 10.1109/ICEngTechnol.2017.8308186.

[20] K. Simonyan and A. Zisserman, "Very Deep Convolutional Networks for Large-Scale Image Recognition." 2014 [Online]. Available: http://arxiv.org/abs/1409.1556

[21] K. He, X. Zhang, S. Ren, and J. Sun, "Identity mappings in deep residual networks," *Computer Vision – ECCV 2016*, pp. 630–645, 2016.

[22] F. Chollet, "Xception: Deep learning with depthwise separable convolutions," *2017 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 2017.

[23] M. Tan and Q. V. Le, "EfficientNet: Rethinking Model Scaling for Convolutional Neural Networks.," in *ICML*, 2019, vol. 97, pp. 6105–6114 [Online]. Available: http://dblp.uni-trier.de/db/conf/icml/icml2019.html

[24] M. Barreno, B. Nelson, R. Sears, A. D. Joseph, and J. D. Tygar, "Can machine learning be secure?," *Proceedings of the 2006 ACM Symposium on Information, computer and communications security - ASIACCS '06*, 2006.

[25] M. Barreno, B. Nelson, A. D. Joseph, and J. D. Tygar, "The security of Machine Learning," *Machine Learning*, vol. 81, no. 2, pp. 121–148, 2010.

[26] Q. Liu, P. Li, W. Zhao, W. Cai, S. Yu, and V. C. Leung, "A survey on security threats and defensive techniques of Machine Learning: A data driven view," *IEEE Access*, vol. 6, pp. 12103–12117, 2018.

[27] D. T. Nguyen, J. K. Kang, T. D. Pham, G. Batchuluun, and K. R. Park, "Ultrasound image-based diagnosis of malignant thyroid nodule using artificial intelligence," *Sensors*, vol. 20, no. 7, p. 1822, 2020.

[28] C. Szegedy *et al.*, "Intriguing properties of neural networks," 2013 [Online]. Available: http://arxiv.org/abs/1312.6199

[29] T. zen, "Thyroid for pretraining," *Kaggle*, 27-Aug-2021. [Online]. Available: https://www.kaggle.com/tingzen/thyroid-for-pretraining. [Accessed: 08-Nov-2022].

[30] IBM, "Adversarial Robustness Toolbox," *Adversarial Robustness Toolbox 1.12.1 documentation*. [Online]. Available: https://adversarial-robustness-toolbox.readthedocs.io/en/latest/index.html. [Accessed: 08-Nov-2022].

Journal of Emerging Computer Technologies
Review Article
Received: *2022-10-12* | ***Reviewing:*** *2022-10-15* & *2022-12-30*| ***Accepted:*** *2022-12-31* | ***Online:*** *2022-12-31* | ***Issue Date:*** *2022-12-31*

ASD Automatic Detection by Using Yolo V3 and Yolo V4 Method

Farah Muwafaq Kamil Alquraishi
Electrical & Computer Engineering
Altinbas University
Istanbul, Turkey
farah89.cs@gmail.com
0000-0001-7481-3280

Mesut Cevik
Electrical & Computer Engineering
Altinbas University
Istanbul, Turkey
mesut.cevik@altinbas.edu.tr
0000-0003-0299-9076

Alzubair Alqaraghuli
Information Technology
Altinbas University
Istanbul, Turkey
zubairsk53@gmail.com
0000-0002-6117-8051

***Abstract*— In this paper, we proposed a deep learning model to classify children as healthy or with autism, accurately (MAP = 88%). Autistic children suffer from social skills and repetitive behaviors in communicating with people or the outside world, although autism is often classified as hereditary, autistic patients have facial features, allowing researchers to analyze children's photos to determine whether they have the disease or not. Where the image is translated into words and numbers using YOLO v3, v4. YOLO is one of the modern methods used in detecting things, especially by using convolutional neural networks, which are considered the basis of work especially because of its high speed and accuracy. In this paper, we worked on a data set containing pictures of children with and without autism. This data set contains 2936 number of pictures. After dividing and processing them in terms of intensity of lighting and dimensions, which allows the model to distinguish between images. After training for several times and using the data set, we got good results. were MAP = 88% as an accuracy and current average loss=0.91% and recall=0.85 and F1=0.77.**

Keywords*— *Autism Spectrum Disorder, YOLO, YOLO v3, v4, CNN, Deep learning, Machine learning

I. INTRODUCTION

Communication disorders that occur in the nervous system are called autism spectrum disorders (ASD). It causes many problems, including difficulty in social and intellectual communication, and repetitive behaviours, all of which affect the overall performance of the patient [1][2]. It can also be classified as a developmental disorder, so most symptoms appear in the first or second year of a child's life [3]. Therefore, early detection is an essential and important part of reducing symptoms or controlling them later [4]. There are a number of factors that must be taken into account when classifying autism, the most important of which are:

A. Males are more likely to have autism than females

B. Having a brother or sister with autism

C. Parents may be elderly (mother over 35 years old) or (father over 40 years old)

Genetics are also important in the risk of developing autism [5].

Machine learning and deep learning are used to diagnose disorders not only autism, but also ADHD. This rapid development of algorithms saves a lot of time to obtain the required services.

Here, a model of the convolutional neural network of deep learning CNN will be implemented, especially because this algorithm has the possibility of classifying neurological diseases [6]. We will use the object detection technology called YOLO. This technique detects objects through images or video clips. This algorithm depends in the nature of its work on the principle of regression, that is, it analyzes and predicts the categories in the entire image [7]. YOLO is characterized by the speed of detecting objects or objects, in order to bypass the work of R-CNN in terms of artwork [8]. The classification of the autism spectrum was based on questionnaires previously, and this may be incorrect in most cases, so here we suggest using a set of images of children with and without autism, using CNN deep learning algorithms, and applying object detection technology, which is the best in detecting autism[9][10]. We now have a set of pictures of children with and without autism. There are many features that we have to consider when applying the algorithm, especially with regard to facial features. A child with autism has a wide upper face and wide eyes, and also the middle area is shorter than the face to include the cheeks and nose [11].

II. THEORY

A. Object Detection

A scientific field that contains many disciplines, the main work of which is the processing and understanding of computers, i.e. images and video clips, the possibility of facial recognition, as well as image retrieval [12]. It not only detects the object, but also determines its location. It is used in many areas, including facial recognition systems in mobile phones, as well as traffic lights and car movement, etc. [13].

B. Convolutional Neural Networks (CNN)

One of the deep learning techniques that are used to build models to solve a specific problem similar in its operation to the human brain, it is fed from the front and contains one input and one output layer, and also contains many layers such as the bypass layer, the assembly layer and other connected layers [14]. The convolutional neural network is the important part of the CNN that is used in the model to extract the required features and train the layer on basic features such as edges and lines to then extract squares and features to include the face, eyes and nose [15]. Below, as shown in Figure 1 there is a simple architecture of CNN and its structures.

Cite (APA) : Muwafaq Kamil Alquraishi, F., Cevik, M., Alqaraghuli, A. (2022). ASD Automatic Detection by Using Yolo V3 and Yolo V4 Method. *Journal of Emerging Computer Technologies*, 2(2), 48-51.

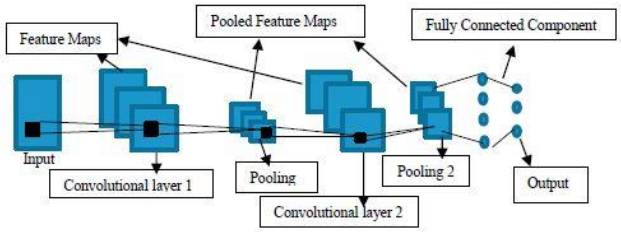


FIG.1. BASIC STRUCTURE OF A CNN MODEL[14]

C. You Only Look Once

This algorithm is used in the field of computer vision, where it can classify objects within the image (dogs, cats, cars, etc.) and also determine the location of the object within the image[7] YOLO. You are only looking at once. A convolutional network is making predictions many times at the same time.

YOLO trains on the full image so that the object is detected directly. The most important characteristic of this algorithm is the speed and accuracy in detecting objects[16]. Figure 2 is a simple architecture of the YOLO structure.

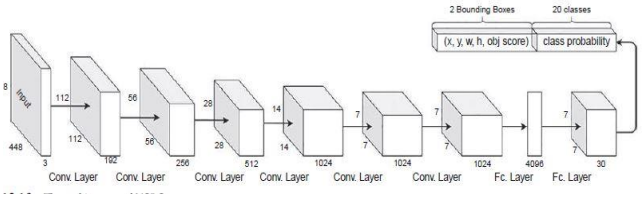


FIG.2. THE ARCHITECTURE OF YOLO[17]

D. Yolov4

This model is used to detect objects. It was developed in 2020 to become more rapid and accurate in its work. Its work depends on the CNN convolutional neural network, where the network divides the image into a number of regions and then predicts the boundary boxes for each region.

YOLO v4, what happens here is the fragmentation of the model that is used in the research into three parts.

- The part of the spine, which is responsible for extracting the features in the input images
- The part of the neck that generates the pyramid of discrimination
- The header part, which is the last and gets its features from the previous part. It also predicts the bounding box area and the category associated with it [10][18].

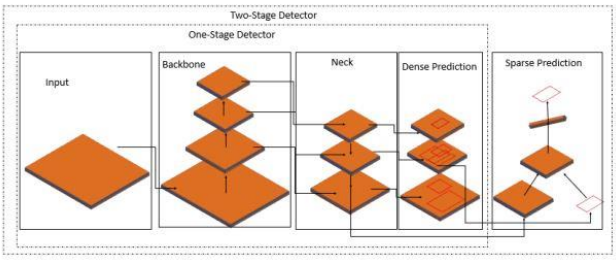


FIG.3. YOLOV4 NETWORK STRUCTURE [19]

III. DESIGN

Children with autism are characterized by special facial features and also the difference between the distance between the features of the face.

Here, we propose a model based on extracting autism through the precise features of the face. The basis of this study is the CNN convolutional neural network and the YOLO algorithm, i.e. object detection.

The most important characteristic of a convolutional neural network is its ability to extract features through CNN layers [20].

FIG.4. SAMPLE INPUT DATA SET

A. Dataset

- *Image Collecting*

In this research, we have used a data set that everyone can use. We obtained it from the Git Hub website. This data consists of 2936 images divided into children with autism and children without autism.

TABLE I. DATASET SPECIFICATION

SPECIFICATION	VALUE
Resolution	1920*1080
Extension	.JPG
Number of Images	2936
Number of class	2
Image size	900-1000 kb

- *Image labelling*

We give each image or category a user name or a so-called(label image)through the (Labelling) program Who draws a square around the object to be discovered and gives five values for this object divided into A value or number for the class and two values X and Y represent the location of the object and the rest of the values are for the size of the object

These values will then be saved to the (XML) folder. As in the Figure 3, this process continues for each image used and for all class.

FIG 5. IMAGE LABELLING USING LABELIMG

B. Model Training and Results

- *Platform*

In the presented study, it is used Windows 11 system, and PyCharm environment, also python 3.7. is used under the Darknet framework, the YOLOv4 algorithm is applied. NVIDIA RTX 3070 graphic card is used to accelerate training and the processor is Ryzen 7 5800H.

- *Training*

The form is used a number of times to get the best results. The model is trained on 2000 times of repetition. More steps of iteration does not mean better results. In the beginning, the training was done directly on the data, but this was not good, so we made some adjustments to the data set In the first training for 1000 times. Of the repetitions, the accuracy was 19% to reach 85%, with a lower loss rate, as shown in the figure below.

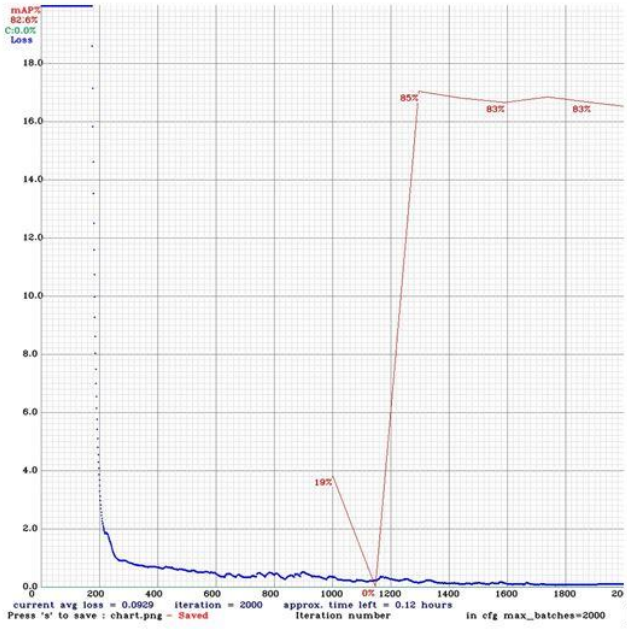


FIG.6. FIRST TRAINING

Then we used Yolo 4 and with the same number of repetitions 2000 times, we will notice an increase in accuracy and a decrease in the average where the accuracy reached 89% and the percentage of the average loss 0.915 as shown in the figure below.

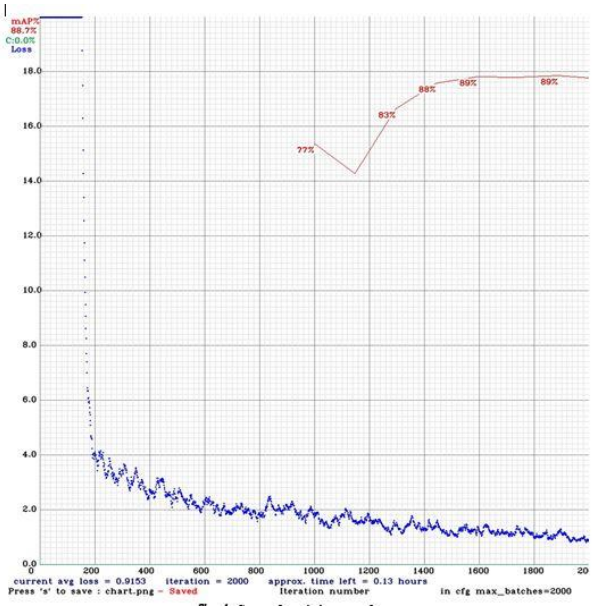


FIG.7. SECOND TRAINING

C. Result

We can say that we have obtained satisfactory results, and the classifier that we trained can be used in diagnosing children with autism, meaning that it was able to identify children's faces and determine the possibility of autism or not.

As in the pictures below, which shows the affected child and the child without autism.

FIG.8. AUTISM CHILD

FIG. 9. NON-AUTISM CHILD

We can summarize the results that appeared to us in the first and second training and display them here through the Table II.

TABLE II. Last Trainings Results

Results	First training	Second training
precision	0.69	0.70
recall	0.88	0.85
F1-Score	0.77	0.77
TP	234	214
FP	106	32
FN	31	39
Average IOU	56.85%	63.90%
MAP	85.19%	85.49%

IV. CONCLUSION

In this research, a model was made to identify children with autism by using a data set of facial images using Yolo v4. The model got 89% MAP As a very good accuracy and average loss 0.91% In the future, we will work on using more data set, and we will also use video clips, and we will also be keen to increase the accuracy of the images used in the data set.

REFERENCES

[1] E. Honey, J. Rodgers, and H. McConachie, "Measurement of restricted and repetitive behaviour in children with autism spectrum disorder: Selecting a questionnaire or interview," Res. Autism Spectr. Disord., vol. 6, no. 2, pp. 757–776, 2012.

[2] M. A. Just, V. L. Cherkassky, A. Buchweitz, T. A. Keller, and T. M. Mitchell, "Identifying autism from neural representations of social interactions: neurocognitive markers of autism," PLoS One, vol. 9, no. 12, p. e113879, 2014.

[3] N. Hasan and M. J. Nene, "An Agent-Based Basic Educational Model for the Children with ASD Using Persuasive Technology," in 2022 International Conference for Advancement in Technology (ICONAT), 2022, pp. 1–6.

[4] J. H. Elder, C. M. Kreider, S. N. Brasher, and M. Ansell, "Clinical impact of early diagnosis of autism on the prognosis and parent–child relationships.," Psychol. Res. Behav. Manag., 2017.

[5] J. Baio et al., "Prevalence of autism spectrum disorder among children aged 8 years—autism and developmental disabilities monitoring network, 11 sites, United States, 2014," MMWR Surveill. Summ., vol. 67, no. 6, p. 1, 2018.

[6] P. Mazumdar, G. Arru, and F. Battisti, "Early detection of children with autism spectrum disorder based on visual exploration of images," Signal Process. Image Commun., vol. 94, p. 116184, 2021.

[7] M. J. Shafiee, B. Chywl, F. Li, and A. Wong, "Fast YOLO: A fast you only look once system for real-time embedded object detection in video," arXiv Prepr. arXiv1709.05943, 2017.

[8] J. Redmon, S. Divvala, R. Girshick, and A. Farhadi, "You only look once: Unified, real-time object detection," in Proceedings of the IEEE conference on computer vision and pattern recognition, 2016, pp. 779–788.

[9] M. F. Rabbi, S. M. M. Hasan, A. I. Champa, and M. A. Zaman, "A convolutional neural network model for early-stage detection of autism spectrum disorder," in 2021 International Conference on Information and Communication Technology for Sustainable Development (ICICT4SD), 2021, pp. 110–114.

[10] A. Bochkovskiy, C.-Y. Wang, and H.-Y. M. Liao, "Yolov4: Optimal speed and accuracy of object detection," arXiv Prepr. arXiv2004.10934, 2020.

[11] Z. A. T. Ahmed et al., "Facial Features Detection System To Identify Children With Autism Spectrum Disorder: Deep Learning Models," Comput. Math. Methods Med., vol. 2022, 2022.

[12] L. Guan, Multimedia image and video processing. CRC press, 2017.

[13] J. Wu, A. Osuntogun, T. Choudhury, M. Philipose, and J. M. Rehg, "A scalable approach to activity recognition based on object use," in 2007 IEEE 11th international conference on computer vision, 2007, pp. 1–8.

[14] S. Raj and S. Masood, "Analysis and detection of autism spectrum disorder using machine learning techniques," Procedia Comput. Sci., vol. 167, pp. 994–1004, 2020.

[15] J. Du, "Understanding of object detection based on CNN family and YOLO," in Journal of Physics: Conference Series, 2018, vol. 1004, no. 1, p. 12029.

[16] A. Kumar, A. Kalia, and A. Kalia, "ETL-YOLO v4: A face mask detection algorithm in era of COVID-19 pandemic," Optik (Stuttg)., vol. 259, p. 169051, 2022.

[17] S.-C. Huang and T.-H. Le, Principles and Labs for Deep Learning. Academic Press, 2021.

[18] J. Yu and W. Zhang, "Face mask wearing detection algorithm based on improved YOLO-v4," Sensors, vol. 21, no. 9, p. 3263, 2021.

[19] A. Alqaraghuli and A. T. A. Oğuz, "Optimized YOLOv4 Algorithm for Car Detection in Traffic Flow," Turkish J. Sci. Technol., vol. 17, no. 2, pp. 395–403, 2022.

[20] N. Kaur, V. KumarSinha, and S. S. Kang, "Early detection of ASD Traits in Children using CNN," in 2021 2nd Global Conference for Advancement in Technology (GCAT), 2021, pp. 1–7.

Journal of Emerging Computer Technologies
Research Article
Received: *2023-02-08* | ***Reviewing:*** *2023-02-08* & *2023-02-15*| ***Accepted:*** *2023-02-15* | ***Online:*** *2023-02-19* | ***Issue Date:*** *2022-12-31*

A New Dynamic Supplier Selection and Supplier Evaluation Model in a Company for Decision-Making Process

Pınar AZİMLİ
Dokuz Eylül University
The Graduate School of Natural and Applied Sciences
Department of Computer Engineering
İzmir, Turkiye
pinar.azimli@ogr.deu.edu.tr
0000-0002-0824-2456

Yalçın ÇEBİ
Dokuz Eylül University
Faculty of Engineering
Department of Computer Engineering
İzmir, Turkiye
yalcin@cs.deu.edu.tr
0000-0002-2330-4440

***Abstract*— Supplier selection and evaluation processes are the companies' most critical decision-making processes. To achieve the desired customer satisfaction, selecting the most suitable supplier and evaluating the suppliers with objective criteria and scientific methods is essential. Supplier Selection (SS) is a strategic decision that a company implements when searching for a new supplier. In contrast, Supplier Evaluation (SE) refers to selecting suppliers among their existing suppliers. As criteria and weights are different in the supplier decision of the companies, a flexible and extensible model called the Dynamic Supplier Analysis Model (DSAM) is developed. This model enables the creation of criteria groups under SS and SE templates, assigning weights to criteria, and applying Multi-Criteria Decision-Making (MCDM) methods. A software program, Dynamic Application for Supplier Analysis Model (DAppSAM), is developed to implement the DSAM model in one of the world's leading chemical companies using an Enterprise Resource Planning System (ERP) as a case study. Decision-Making Trial and Evaluation Laboratory (DEMATEL) method is applied to calculate criterion weight using dependencies and relationships between criteria. The Analytical Hierarchy Process (AHP) and Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS) MCDM methods were applied using a quality advantage SE template to select materials. The confirmed results by experts show that this model allows companies to analyze their suppliers efficiently.**

Keywords*— *Supplier Selection, Supplier Evaluation, MCDM, AHP, TOPSIS

I. INTRODUCTION

Supplier defines any person, business, institution, or organization that supplies goods or services to companies. The term "supplier identification" is the process of determining which suppliers will supply goods and services to companies according to their fields of activity. Since customer satisfaction is at the center of business decisions, companies are trying to cooperate with suppliers to satisfy their customers. In today's competitive business environment, finding suitable suppliers has become more critical due to the increasing costs and low-profit figures. For this reason, businesses need a supplier determination system that enables them to establish long-term relationships with their suppliers by selecting the most suitable suppliers according to their expectations and goals, reviewing these relationships in specific periods, and managing their suppliers [1].

A purchasing expert is an individual who has a critical role during the supplier decision process. Purchasing experts manage all the purchasing processes of a business, negotiating with vendors to get the best price for goods and services. And also, it is important to communicate with other departments and company employees and take care not to exceed the budget limits while making their purchases.

Since a supplier can be chosen among new candidates or existing suppliers, the supplier determination can be classified into two processes: Supplier Selection (SS) and Supplier Evaluation (SE). The SS process is the process of identifying a supplier among candidate suppliers. Therefore, SS is the cornerstone for strategic sourcing and procurement advantage, and the decision-making process during this selection is accepted as strategic. In SS, data is obtained from suppliers through surveys and interviews, so collected data is unstructured. However, these unstructured data must be converted into structured data to be used in the evaluation process. And also, if the collected data format is unstructured, then the ability of the decision-maker to decide quickly with the required precision is hampered [2].

In contradistinction to the SS, the SE process is carried out on the current suppliers of the company. This process helps companies to evaluate their existing suppliers in order to decrease the purchasing risk and maximize the overall value to the buyer. The SE process is intended to guarantee that the best supplier is available. In the SE process, both the data obtained from the ERP of the company and the data collected from purchasing experts are used. Therefore, the SS process is accepted as a strategic decision-making process, the SE process is recognized as a tactical and operational decision process [3].

Criteria are the plural form of the word criterion, which describes a standard, rule, or test on which a judgment is based. In the past, companies used to make supplier decisions by considering price criteria, but with the increasing competition, different criteria, such as quality control certificates, customer complaints, capacity, and capability, were considered for evaluating alternatives. However, the companies may evaluate suppliers for different material and service purchases by defining the criteria and criterion weights according to their requirements. In this way, companies operating in different industry areas can evaluate

Cite (APA) : Azimli, P., Çebi, Y. (2022). A New Dynamic Supplier Selection and Supplier Evaluation Model in a Company for Decision-Making Process. *Journal of Emerging Computer Technologies*, 2(2), 52-60.
Volume:2, ***No***:2, ***Year:*** 2022, ***Pages:*** 52-60, December 2022, *Journal of Emerging Computer Technologies*

existing suppliers and choose new suppliers according to their objectives.

In this study, a new model and software are developed to provide a solution to supplier decisions of companies in different industry areas by applying MCDM methods with a dynamic system structure. The supplier selection and evaluation processes can be distinguished by defining criteria and templates based on the requirements of a company. Decision-makers can define criteria and the calculation method to determine the criterion values of suppliers in this software. Moreover, criteria can be selected, and weights of criteria are assigned under template structures according to the requirements of the company. The weights of the criteria can be calculated after defining the effects and importance of the criteria. It is intended to integrate existing supplier data with an ERP system for the SE process. The suppliers are evaluated with more realistic data with this integration. Additionally, a structure is essential where different MCDM methods can be included and applied to supplier decisions. Therefore, a dynamic model should be established to identify and classify SS and SE criteria for selecting a supplier and to apply appropriate MCDM methods based on the industry domain.

II. Literature Review

Due to the importance and widespread use of Supplier Selection (SS) and Supplier Evaluation (SE) processes in many fields, numerous studies have been found in the literature. A novel grey decision model to evaluate suppliers for the process industry [4]. Analytic Network Process-Technique for Order of Preference by Similarity to Ideal Solution (ANP-TOPSIS) method is applied in the automotive industry for evaluating suppliers [5].

A multi-criteria intuitionistic fuzzy TOPSIS method sustainable supplier selection and determine the rank of suppliers through a real-world case study [6]. A model is constructed for integrated supplier selection by applying the ANP, Taguchi loss function, and PROMETHEE methods. In this study, various criteria were determined, such as price, delivery, financial status, and management capabilities. They used the ANP methods to determine criterion weights and relationships, Taguchi Loss Function, and PROMETHEE approaches to find the best supplier, rank the suppliers and apply in Tire Company. In conclusion, precise solutions were determined for complicated selection problems with traditional and non-traditional methods comparatively [7]. The generalized Choquet integral and the fuzzy TOPSIS approaches are applied to select the best supplier for purchasing steering gearbox products for the automotive industry in Turkey. The results showed that the fuzzy MCDM methods provided more reliable solutions instead of traditional MCDM methods [8].

Supplier decisions are made using the SS and SE criteria in conjunction with MCDM methods. The criteria are set by the companies based on their goals in selecting a product or service and applying MCDM methods [9]. Moreover, in the study of a company producing corrugated cardboard boxes in Turkey, the most frequently used criteria for supplier selection were price, quality, delivery, service, and sub-criteria. The weights of the criterion are determined by the Analytical Hierarchy Process (AHP) method, and alternative suppliers were selected with the TOPSIS method [10]. A literature review of supplier criteria selection and the research trends on criterion selection based on a review of related studies for selecting suppliers is presented. Also, the AHP method is applied in the business sector to gain optimal results [11]. The suppliers are selected, and supplier development status is found with the TOPSIS method [12].

The AHP and TOPSIS methods were used for housing selection [13], the measurement of corporate sustainability in the bank sector [14], and the evaluation of polyclinics [15]. A comprehensive evaluation model based on VIKOR and TOPSIS models is proposed to determine the security status of urban water supplies. The results indicate that Tianjin should develop water resources and focus on the construction of a water-saving society [16].

In a study, the rankings obtained by the TOPSIS and VIKOR methods, which are multi-criteria decision-making techniques, were compared in order to make the financial performance rankings of the enterprises. They examined whether there is a relationship between their financial performance and stock market performance by sequential correlation analysis [17].

The Grey Relational Analysis (GRA)-Best Worst Method (BWM-TOPSIS methods are integrated to propose a framework for resilient supplier selection with the presence of uncertain and incomplete data [18].

The decision-making trial and evaluation laboratory (DEMATEL) and Analytical Network Process (ANP) methods were used together for supplier selection in the health sector. The criteria are ranked as price, quality, sustainability, OHS, technique, and logistics with these methods. It is indicated that the proposed method may help managers with purchasing decisions [19]. They propose a methodology by using PROMETHEE II that identifies the best criteria first and calculates the preference indices according to these criteria. The PROMETHEE II algorithm is customized, and statistical analysis indicates that the proposed approach might be applied instead of PROMETHEE II and TOPSIS methods [20].

The effect of the criteria on supplier selection for bottleneck and strategic product groups is discussed. The bottleneck products have a particular design, while strategic product producers are limited. There are three candidate suppliers for each group. Criteria and sub-criteria with their weights were defined according to product groups. In this study, it was given that the criteria and weights used in supplier selection varied depending on the product group. Furthermore, it was noted that there might be dependencies between the criteria used for supplier selection, and ignoring these dependencies which would lead to erroneous results [21]. Additionally, the criterion “cost” is critical, but the criteria of “performance” and “ease of use” are also determined as essential when selecting a machine in the cable industry. The fuzzy structure enables the decision-makers to evaluate statements and create an objective decision structure [22]. In addition, Fuzzy logic is used to evaluate marble extraction methods [23]. MCDM methods combined with the fuzzy logic to deal with uncertainties by the Fuzzy TOPSIS

method [8] and [24]. Also, Fuzzy TOPSIS and Fuzzy DEMATEL were used by [25] to select the most suitable supplier. Similarly, the criteria weights and relationships are determined by using the Fuzzy DEMATEL technique [26] and [27]. Besides, the fuzzy AHP method is applied to determine the best alternative and the most suitable machine suppliers [28].

Also, another MCDM algorithm, namely Data Envelopment Analysis (DEA) is used to calculate relative importance and to monitor market performance by using many inputs and outputs without calculating weights [29]. The Analytical Network Process (ANP) to determine the weight in supplier selection criteria and the DEA method to handle hundreds of suppliers Reference [30]. Besides, supplier selection in the cable industry by employing the DEMATEL method for determining criteria relations, the ANP method for determining criteria weights, and the VIKOR method for supplier selection. In the cable industry, DEMATEL, Analytic Network Process, and VIKOR method are used to select polyethene suppliers [31,32]. As a result, "the suitability of the product price" is found as an essential criterion, and two companies are identified as the best suppliers. Additionally, the Delphi technique may also be used when individuals and groups need to solve complex problems without face-to-face meetings [33]. A comprehensive solution model is developed to select supplier in the Oil and Gas (O&G) industry to prevent delay problems during O&G operations resource extraction. They applied a Delphi technique to filter unnecessary factors and rank factors. Moreover, the best-worst method (BWM) is applied to calculate the weights of criteria and reduce pairwise comparisons. TOPSIS method is implemented to rank the suppliers. The applicability of this integrated MCDM model in the O&G industry reveals that this model can be used in other industrial sectors for SS [34].

Besides, Principal Component Analysis (PCA) is used to reduce the dimensionality of large datasets by computing low-dimensional representations of multivariate data [35] and [36]. Medium-sized bottling machine companies have used this method to evaluate the relative performance of suppliers with multiple outputs and inputs [37].

The fuzzy TOPSIS approach is applied to select hospital suppliers for ten main and twenty-four sub-criteria to evaluate three hospital supplies. Supplier one is selected as the best sustainable supplier but supplier two has the best performance based on economic criteria in the study. They indicate that this work can help hospital managers make decisions on candidate suppliers [38].

III. Problem Definition

Many other studies can be found which are carried out for different sectors in supplier decisions. The studies are sector-specific and inflexible with fixed criteria and methods. In the previous studies, it was seen that the concepts of SS and SE are intertwined. Besides, to the best of the authors' knowledge, no study exists that defines SS and SE processes separately and also has a flexible and extensible model depending on the company. Thus, companies can meet their expectations by defining their criteria within a model that provides e.g. financial, operational, and cost benefits. Also, another significant problem in evaluating criteria for SS and SE process is data collection methods. The companies are unclear about the required data, its format, the methods for collecting the data and collected data is unstructured form. In this model, an unstructured data should be converted into structured data. Regarding the mentioned problems, companies should determine the nature, definition, and use of data in the supplier selection and evaluation process.

IV. Methodology

A. Model Definition

In this paper, a novel, flexible and extensible model for both SS and SE called Dynamic Supplier Analysis Model (DSAM) is developed. DSAM model consists of four phases which are Data Collection and Preparation, Method Development, Evaluation, and Analysis shown in Fig. I.

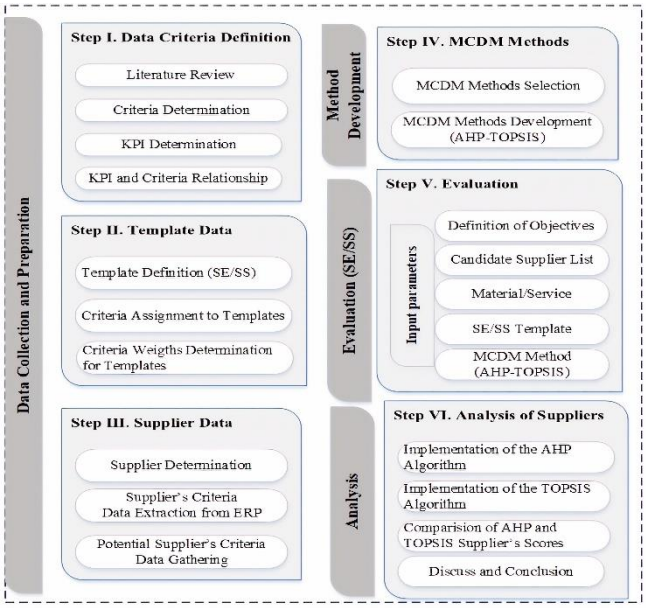


FIG I. DSAM MODEL

Data Collection and Preparation phase is the most important phase of this model. In the criteria creation step of this phase, literature analysis and workflow analysis of different firms were carried out, and criteria found after this research was analyzed by experts.

The criteria "Quality Control", "Product Control", "Delivery Performance", "Customer Complaints ", "Price and Payment Terms Control", "Accuracy" and "Quantity Control" were defined as follows;

Quality Control; Accepted ratio and Rejected products ratio

Product Control; the ratio of correct and incorrect product gives the result value of this criteria.

Delivery Performance; the performance of supplier for Order Delay Date, Packaging Capability and distance

Customer Complaint; the count of complaints gives the score for a supplier.

Price and Payment Terms Control; Ratio of Correct Price, correct payment term and Out of Tolerance criteria are used to calculate supplier value.

Accuracy; criteria value is calculated by the ratio of ontime delivery, correct product and amount of a material that is purchased

Quantity Control; the ratio of correct and out of tolerance gives the value of the criteria for a supplier.

For each of the criteria, KPI's value definition methods were determined. After this step, different templates were defined to give flexibility and manageability to the user, and a hierarchical criteria tree, including weights for each criterion. In the Supplier Data step, different approaches were applied to the existing supplier or candidate supplier. For existing suppliers, data, criteria, and KPI values that exist in the ERP System of the company are imported. For candidate suppliers, their required data, criteria, and KPI values are obtained in digital form if possible or the required data is entered into the system manually.

The well-known and most used methods, AHP and TOPSIS, are developed in the Method Development phase. And also, depending on the requirements of the company, new methods can easily be applied and integrated into the system. Moreover, in the Evaluation phase of the model, the requirements of the company are determined, the materials and services are selected to be purchased, and SS and SE processes are carried out. In this phase, the user can select the suitable template for any desired situation, such as quality advantage, cost advantage, minimum price, and delivery time. The user also can define new templates according to their requirements. The Analysis is the last phase of the presented model, in which the results obtained from the applied methods are combined to make the final decision after the necessary analyses by the experts.

B. Data Collection and Analysis

The most important step in the data collection is determining the criteria. First, the criteria list is populated from the previous studies carried out by the different authors in the literature and the analysis carried out on different firms. Then each criterion was discussed with the purchasing experts, and then final criteria list was created. Values of the criteria can be determined by using two different ways depending on the situation of the current suppliers and candidates. For current suppliers, criteria values are determined depending on the data in the ERP system of the company. For candidates, the data used for the value determination is collected from surveys and interviews with the suppliers. Then, three data preparation techniques are performed together to extract meaningful information from the raw data, including (i) Criteria Determination Processes: New Criterion Adding Processes, Criterion Splitting Processes, Criteria Merging Processes, and Criterion Removal Processes. (ii) Segmentation: Criteria Characteristics Definition. (iii) Feature Extraction: Grouping Criteria as SS/SE and defining a related scale. Finally, the experts in the company finalize the criteria values and weights to be used during SS and SE processes.

C. The Relation between Criteria and KPI

KPI structure provides to define the method of obtaining the criteria values of the suppliers and the criterion scale ranges. The working methods of the criteria are determined by the KPI type and the calculation method. Also, KPI scales determine the actual value of the interval for scores and the direct effect of a criterion value. Some detailed examples of the KPI with scale and its intervals are given in Table I.

TABLE I. KPI DETAILS

KPI ID	KPI Name	Criterion Name	Method	Data	Scale	Unit	The effect	Interval	Score
69	Order Delay Time	Order Delay Time	Function	Transaction Values	15	Day	The negative effect Max Day=Min Score	-30 day -30/-10 -10/0 0/5 5/	5-Perfects 4-Good 3-Normal 2-Acceptabl 1-Bad
448	Distance	Distance	Objective Data Method	Data	95	Km	Negative Effect Max Distance=Min Score	Distance Min/Max Interval	1-Good, 2-Normal 0-Bad 3-Perfect
449	Packaging Capability	Packaging Capability	Subjective Data Method	Data	94	Bool	Exists Max Score	1-Exist 0-NotExist	1 0

D. Templates

Templates are criteria groups created to select or evaluate a supplier for a product or service. A template also gives the ability to users to define their requirements by using KPI and KPI weights in the system. While creating the templates, the Year, the Type (SE/SS), and the features of the template are selected. The features include "Cost", "Delivery", "Quality", and "Quantity", as given in Table II. These features enable to distinguish templates easily without reviewing KPI details. The user may also select one or more of these features depending on the requirements.

TABLE II. QUALITY ADVANTAGE TEMPLATE PROPERTIES

	Year	*Type*	*Cost*	*Delivery*	*Quality*	*Quantity*
Quality Advantage	2012	SE	☐	☐	■	☐

Each template has layers in which a sub-criteria is defined for each main criterion in a top layer. After adding criteria to the templates, weights are assigned to each criterion. These weights can be determined by experts or can be calculated using a method. In Table III, the Quality Advantage Template was created by experts; the first two layers of this template are given. As can be seen in Table III, the overall sum of the

weights defined in each layer is 100%, while each criterion has its weight. The weight of the criterion can be assigned under the template based on requirements. Besides, the weight of the criterion can be calculated by Decision-Making Trial and Evaluation Laboratory (DEMATEL) method in this model. The DEMATEL method determines the type of relations, the importance of the criteria, and their effects on each other [39] and is applied to determine criteria and criteria weights by using evaluation scales. These scales are linguistic terms as No influence, low influence, Medium influence, high influence and very high influence [40].

TABLE III. SE RESULTS OF THE AHP METHOD FOR QUALITY ADVANTAGE TEMPLATE OF TWO LAYERS

QUALITY ADVANTAGE TEMPLATE MAIN/SUB CRITERIA (LAYER I, LAYER II)			
LAYER I		**LAYER II**	
Criterion	**W%**	**Criterion**	**W%**
Quality Control	30%	Accepted Ratio	30%
		Condional Accepted Ratio	30%
		Environment Related Cerificates	20%
		QDMS System	20%
Product Control	15%	Ratio of Correct Product	40%
		Quality Control	60%
Delivery Performance	10%	Order Delay Date	50%
		Packaging Capability	20%
		Distance	30%
Price and Payment Terms Control	15%	Payment Control	50%
		Price Control	50%
Customer Complaints	5%	Quality Complaints	50%
		Delivery Complaints	10%
		Packaging Complaints	10%
		Handling of Complaints	20%
		Price Complaints	10%
Accuracy	10%	Ratio of Correct Price	13%
		Delivery On-Time Ratio	15%
		Delivery Correct Product	50%
		Delivery Amount Accuracy	12%
		Proper Packaging	10%
Quantity Control	15%	Ratio of Correct Quantity	80%
		Waste Rate	20%
Sum (Layer I)	**100%**		

The criteria to be used in the evaluation process are selected among the existing criteria in the system. In this selection process, the opinions of experts are taken, and the decision-makers can compare the relationships among the criteria by using criterion evaluation scales. Moreover, the DEMATEL method is applied to calculate criterion weight by using dependencies of criteria [41, 42]. In this study, Quality Control, Product Control, Delivery Performance, Price and Payment Terms Control, Customer Complaints, Accuracy, and Quantity Control criteria weights are calculated as 0.17814, 0.16888, 0.08867, 0.18084, 0.16676, 0.13601, 0.08071. These values indicate that price and payment terms control criteria are very important criteria. This template is created as a quality advantage, so the quality control criterion weight is assigned as 30%. However, the prerequisite of 100% total should always be preserved.

E. MCDM Methods

It is determined that different MCDM methods are used in supplier decision-making in the literature examined within the scope of this study. In this work, the Analytical Hierarchy Process (AHP) and Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS) methods are used to calculate supplier score values. AHP method is a mathematical theory that is the most popular and widely used multicriteria method in decision-making developed by [38]. The criteria are compared according to their priorities, and criteria weights and supplier scores are calculated using the AHP method. On the other hand, the TOPSIS method is one of the MCDM methods frequently used in the selection of suppliers in literature [43]. The scores of the alternatives are considered by calculating the distances between the positive and negative ideal solutions in the TOPSIS method. The selected alternative is expected to be close to the positive ideal solution and away from the negative ideal solution [44].

An algorithm is developed using the analytic hierarchy process (AHP) method to evaluate suppliers. Supplier scores are calculated with the procedures developed for the application of this method. Moreover, the TOPSIS evaluation method is used in this study based on supplier data to evaluate suppliers. In this study, a flexible data structure was created, AHP and TOPSIS methods were applied by the prepared procedures, and the dependency on any ready-made library was eliminated with the development of the procedures within the scope of the study. These procedures allow flexible application of methods for different criteria and alternatives. The AHP method allows the evaluation of alternatives with paired comparison matrices created for the determined criteria. Simple mathematical operations are used in this evaluation process. In this study, the AHP method was used effectively by creating a dynamic data structure and pairwise comparison matrices for both criteria and alternatives. For the application of the method, the procedures developed in the study and the alternatives were evaluated by solving mathematical operations and pairwise comparison matrices. In addition, since the effect direction of the criteria can be positive or negative, the effect aspect of the criteria should also be taken into account in the evaluation of alternatives. If the cost criterion value of an alternative is large, this alternative should be evaluated negatively, and an alternative with minimal cost should be chosen as the best solution. If we consider another criterion, the quality criterion, it will have a positive effect if an alternative has a quality certificate. In other words, the cost criterion has a negative effect, but the quality certificate criterion has a positive effect. The TOPSIS method was used in this study because it calculates the distance of the alternatives from the positive and negative ideal solutions by taking into account the positive and negative effects of the criteria. In addition, to apply the TOPSIS method, a procedure was developed using the flexible data structure used in the AHP method, and mathematical operations were applied with matrix operations. In this way, the evaluation of alternatives was ensured by taking into account the positive and negative effects of the criteria.

In order to calculate supplier score values, the DAppSAM software user interface is shown in Fig. II. Industry field, template, material, and method are selected as parameters,

supplier evaluation and selection are selected, and scores are calculated.

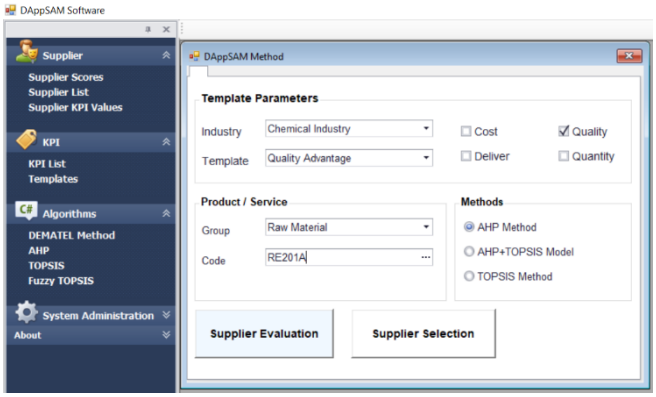


FIG II. DAPPSAM SOFTWARE USER INTERFACE

F. Supplier Score Calculation

AHP and TOPSIS methods are applied using a template, the supplier's data, and KPI value of each supplier is calculated. In order to calculate the supplier score, the criteria score values of suppliers are multiplied by criteria weights depending on the selected template, and a total score is calculated. In each layer, the score of a criterion and the total score of criteria are calculated by using formulas 1 and 2:

$$Score\ of\ criterion\ k = W\%(k) * AR \quad (1)$$

$$Total\ Score = \sum_{i=0}^{n} W\%(i) * AR(\mathrm{i}) \quad (2)$$

Where k= k_{th} criterion

- n: Count of a SS/SE template's main criteria
- W% (k): Weight of the kth criterion on a selected layer
- AR: Result value of a selected algorithm for kth criterion

Score: Multiplication of AR and W% values on a selected layer for kth criterion.

V. RESULTS AND DISCUSSION

The case study was carried out on the data of a chemical company that is among the top five companies worldwide and located in Turkey. The developed software DAppSAM was also integrated with the ERP system of the mentioned company to implement the DSAM model. As given above, the AHP and TOPSIS methods were selected and implemented in this study. Since the processes carried out for both SS and SE are similar, in order to see the effectiveness of the model and to compare with it the real-world data, only the SE was carried out. Also, the ERP data used in this study was related to the last five years. Depending on the purchase orders of the company in these years, 20 current and candidate suppliers were selected from the historical purchase order data at the same time for a product group. In this case study, the Quality Advantage Template was selected for SE. The name of the materials and the name of suppliers were coded to maintain data security. The suppliers have the ability to provide the materials coded as RE201A that were selected and used in the comparisons. The score of each supplier was calculated as given in formulas 1 and 2. The overall scores of the supplier evaluation process carried out by the AHP and TOPSIS methods are given in Tables IV and VI, respectively.

TABLE IV. SE RESULTS OF THE AHP METHOD

Supplier Code	Total Score	Quality Control	Quantity Control	Product Control	Price and Payment Terms Control	Delivery Performance	Accuracy	Customer Complaints
	100%	**30%**	**15%**	**15%**	**15%**	**10%**	**10%**	**5%**
S02	**6.4489**	1.7658	1.1251	1.1107	0.7399	0.5457	0.6724	0.4893
S12	**6.2040**	1.7658	1.1251	1.1107	0.9885	0.3624	0.7536	0.0979
S14	**6.1900**	1.5351	1.1251	1.1107	0.6992	0.5582	0.6724	0.4893
S05	**5.6099**	1.6482	1.1251	0.8494	0.8663	0.3523	0.5993	0.1693
S11	**5.2508**	1.5204	1.1251	0.6888	0.6181	0.4912	0.6788	0.1284
S20	**5.2366**	1.1250	1.0313	0.7943	0.6915	0.5573	0.5968	0.4404
S03	**5.1884**	1.9966	0.2812	0.6888	1.0910	0.4412	0.3176	0.3720
S10	**5.1866**	0.9412	1.1251	0.8494	0.7371	0.6694	0.6462	0.2182
S07	**5.1678**	1.2528	1.0313	0.8494	0.7346	0.5726	0.6507	0.0764
S13	**5.0671**	1.7658	1.1251	0.6888	0.6026	0.5629	0.1720	0.1499
S01	**5.0040**	0.7913	1.0313	0.5330	1.0868	0.4912	0.9011	0.1693
S09	**4.9499**	1.5204	0.1875	1.1107	0.6181	0.5499	0.5149	0.4484
S18	**4.6704**	1.2896	0.2812	1.1107	0.7821	0.4495	0.5880	0.1693
S04	**4.6364**	1.9966	0.2812	0.7943	0.6178	0.3652	0.4529	0.1284
S15	**4.4398**	1.5204	1.0313	0.3723	0.5521	0.3513	0.1720	0.4404
S06	**4.4119**	1.5204	0.1875	0.3723	0.9460	0.8110	0.4463	0.1284
S17	**4.3101**	1.5204	0.2812	0.7943	0.5405	0.5652	0.4392	0.1693
S08	**4.1648**	1.7511	0.2812	0.6888	0.6630	0.3944	0.2364	0.1499
S19	**3.9802**	1.7511	0.1875	0.3723	0.5566	0.5610	0.1633	0.3884
S16	**3.8849**	1.0220	1.0313	0.1110	0.8684	0.3485	0.3264	0.1773
Max. Score	**6.4489**	**1.9966**	**1.1251**	**1.1107**	**1.0910**	**0.8110**	**0.9011**	**0.4893**

Depending on the results obtained, it is observed that supplier S02 has the highest score while supplier S16 has the lowest. When details of the evaluation are examined, it is seen that the order of the suppliers is generally different. For example, suppliers S03 and S04 have the highest scores of 1.9966 from the Quality Control perspective. However, their scores are extremely low when compared to Quantity Control. Supplier S03 has the highest score from the "Price and Payment Control" perspective, but from other perspectives, it is located in the bottom section of the comparison list. Although supplier S02 was detected as the best in overall score, it was not the best in the "Price and Payment Control". In order to show the layer structure, the details of S02 are given in Table V.

After the TOPSIS implementation, it was revealed that supplier S02 is also the most advantageous supplier when the overall score is calculated. Although the supplier "S03" has the highest "Quality Control" score, other criteria scores are lower than it. By considering the overall results for both cases, it is observed that supplier S02 is the first and selected as the final supplier for the material RE201A.

TABLE V. DETAILED RESULTS OF "PRICE & PAYMENT CONTROL" CRITERION FOR SUPPLIER "S02"E RESULTS OF THE AHP METHOD

LAYER								
1		2		3				
Criterion	**W%**	**Criterion**	**W%**	**Criterion**	**W %**	**AR**	**WA% (*)**	**Score**
Price and Payment Terms Control	**15**	**Payment Control**	**50**	Supplier Payment Term	30	3.592	**2.25**	0.0808
				Correct Payment Term	40	4.167	**3.00**	0.1250
				Payment Delay Day	30	3.448	**2.25**	0.0776
				Total	**100**		**7.50**	**0.2834**
		Price Control	**50**	Ratio of Correct Price	40	6.25	**3.00**	0.1875
				Discount percentage by the Amount	40	5.556	**3.00**	0.1667
				Sectorial Price behavior Adjustment	20	6.818	**1.50**	0.1023
				Total	**100**		**7.50**	**0.4565**
		Total	**100**					**0.7399**

TABLE VI. SE RESULTS OF THE TOPSIS METHOD

Supplier Code	Total TOPSIS Score	Quality Control	Quantity Control	Product Control	Price and Payment Terms Control	Delivery Performance	Accuracy	Customer Complaints
	100%	**30%**	**15%**	**15%**	**15%**	**10%**	**10%**	**5%**
S02	24.6167	7.1024	4.2544	4.1810	2.9249	2.1157	2.4021	1.6362
S12	23.7252	7.0579	4.2544	4.1810	3.7676	1.4812	2.6616	0.3215
S14	23.5554	6.1589	4.2544	4.1810	2.7561	2.1667	2.4021	1.6362
S05	21.8870	6.6983	4.2544	3.1371	3.5359	1.4570	2.1686	0.6357
S11	20.2273	6.2084	4.2544	2.6273	2.6340	2.0236	1.9855	0.4941
S03	20.0508	8.0459	1.1470	2.6273	4.1306	1.8196	1.0561	1.2243
S20	19.9726	4.6352	3.8535	3.0158	2.7124	2.1455	2.1319	1.4783
S10	19.9369	3.9174	4.2544	3.1371	3.0002	2.6199	2.2143	0.7936
S13	19.8117	7.1468	4.2544	2.6273	2.4718	2.1682	0.6036	0.5396
S07	19.6309	5.0363	3.8535	3.1371	2.8941	2.2079	2.2260	0.2760
S09	19.3435	6.2972	0.7461	4.1810	2.6340	2.1327	1.8579	1.4946
S01	18.7184	3.1049	3.8535	1.9718	4.0870	2.0236	3.0419	0.6357
S04	18.3535	8.0459	1.1470	3.0158	2.5355	1.4925	1.6227	0.4941
S18	18.2954	5.3093	1.1470	4.1810	3.0774	1.8536	2.0914	0.6357
S15	17.4086	6.2528	3.8535	1.4621	2.3225	1.4358	0.6036	1.4783
S06	17.1779	6.2084	0.7461	1.4621	3.6436	3.3112	1.3124	0.4941
S17	17.1397	6.2528	1.1470	3.0158	2.3058	2.1950	1.5876	0.6357
S08	16.5210	7.1963	1.1470	2.6273	2.6027	1.6115	0.7966	0.5396
S19	15.7532	7.1963	0.7461	1.4621	2.3474	2.1780	0.5631	1.2602
S16	14.8529	4.0928	3.8535	0.4181	3.3154	1.4245	1.0966	0.6520
Max. Score	**24.6167**	**8.0459**	**4.2544**	**4.1810**	**4.1306**	**3.3112**	**3.0419**	**1.6362**

VI. CONCLUSION

In this study, for Supplier Selection and Supplier Evaluation processes a flexible and extensible model named Dynamic Supplier Analysis Model (DSAM) is developed. Moreover, in order to implement the DSAM Model to enable changes in templates and criteria, and to find the optimum solution with commonly used multi-criteria decision-making method TOPSIS and AHP algorithms, an application named Dynamic Supplier Analysis Model (DAppSAM) is also developed. The weights of criteria were calculated by the DEMATEL method and defined under a SE template for the product group in this chemical company. However, the criteria and their weights may differ based on the product group and requirements of a company. The templates structure is used to define the criteria group based on these requirements and revise the weights of crtieria. DSAM model is applied in one of the world's leading chemical companies to determine best supplier for a product group among twenty suppliers. In the DAppSAM software, the scores of these suppliers are calculated for AHP and TOPSIS method. Besides, the impact directions of the criteria is also investigated and it is seen that

the TOPSIS algorithm is also enabled to find the solutions closest to the positive solution and the farthest from the negative solution. Also, by changing the scales' sensitivity, the model can provide more effective solutions. The scores of these methods are consistent for Supplier Evaluation. The supplier S02 is the best supplier with AHP and TOPSIS score values with 6.4489, 24.6167 respectively.

The results are evaluated by experts, and the purchase amount of this product group is analyzed for the years between 2005 and 2011. The supplier "S02" purchase quantity is greater than other suppliers that are evaluated based on quality advantage. Finally, it was seen that DSAM allows companies to analyze their suppliers efficiently. The purchase quantity from all of these suppliers is compared and validated with the scores of suppliers.

REFERENCES

[1] Wu, Z., Choi, T. Y., & Rungtusanatham, M. J. (2010). Supplier–supplier relationships in buyer–supplier–supplier triads: Implications for supplier performance. Journal of Operations Management, 28(2), 115-123.

[2] Agarwal, P., Sahai, M., Mishra, V., Bag, M., & Singh, V. (2011). A review of multi-criteria decision making techniques for supplier evaluation and selection. International journal of industrial engineering computations, 2(4), 801-810.

[3] Monczka, R. M., Handfield, R. B., Giunipero, L. C., & Patterson, J. L. (2020). Purchasing and supply chain management. Cengage Learning.

[4] Pitchipoo, P., Venkumar, P., & Rajakarunakaran, S. (2014). Grey decision model for supplier evaluation and selection in process industry: a comparative perspective. The International Journal of Advanced Manufacturing Technology, 76, 2059–2069.

[5] Shahroudi, K., & Rouydel, H. (2012). Using a multi-criteria decision making approach(ANP-TOPSIS) to evaluate suppliers in Iran's auto industry. International Journal of Applied Operational Research - An Open Access Journal

[6] Memari, A., Dargi, A., Jokar, M. R., Ahmad, R., & Rahim, R. A. (2019). Sustainable supplier selection: A multi-criteria intuitionistic fuzzy TOPSIS method. Journal of Manufacturing Systems, 50, 9-24.

[7] Sarı, T., & Timor, M. (2016). Integrated supplier selection model using ANP, taguchi loss function and promethee Methods. Journal of Applied Quantitative Methods, 11(1), 19-34

[8] Yıldız, A., & Yayla, Y. (2017). Application of fuzzy TOPSIS and generalized Choquet integral methods to select the best supplier. Decision Science Letters, 6(2), 137-150. doi:10.5267/j.dsl.2016.11.001.

[9] Gavade, R. K. (2014). Multi-Criteria decision making: An overview of different selection problems and methods. International Journal of Computer Science and Information Technologies, 5(4), 5643-5646.

[10] Supçiller, A., & Çapraz, O. (2011). AHP-TOPSIS yöntemine dayali tedarikçi seçimi uygulamasi. Istanbul University Econometrics and Statistics e-Journal, (13), 1-22.

[11] Ristono, A., -, P., Santoso, P. B., & Tama, I. P. (2018). A literature review of criteria selection in supplier. Journal of Industrial Engineering and Management, 11(4), 680-696. doi:http://dx.doi.org/10.3926/jiem.2203

[12] Çetinkaya Bozkurt, Ö. (2021). Selecting the Suppliers with TOPSIS and Determining Their Development Status by Using Heuristic Optimization. Acta Infologica, 5(1), 53-64

[13] Alkan, T., & Durduran, S. S. (2020). Analysis of Housing Selection Process with AHP Based TOPSIS Method. Necmettin Erbakan University Journal of Science and Engineering Sciences, 2(2), 12-21. Retrieved from https://dergipark.org.tr/tr/pub/neufmbd/issue/59145/820073.

[14] Oral, C., & Geçdoğan, S. (2020). Kurumsal Sürdürülebilirlik Ölçümü İçin AHP ve TOPSIS Yöntemlerinin Kullanılması: Bankacılık Sektörü Üzerine Bir Uygulama. İşletme Araştırmaları Dergisi, 12(4), 4166-4183

[15] Taş C., Bedir, N., Eren T., Alagaş H. M., & Çetin, S. (2018). AHP-TOPSIS yöntemleri entegrasyonu ile poliklinik değerlendirilmesi: Ankara'da bir uygulama. Sağlık Yönetimi Dergisi, 2(1), 1-17.

[16] Yang, H., Zhang, X., Fu, K. et al. Comprehensive evaluation of urban water supply security based on the VIKOR-TOPSIS method. Environ Sci Pollut Res 30, 8363–8375 (2023). https://doi.org/10.1007/s11356-022-24493-5

[17] Şahin, A., ve B. Sarı, E. (2019). ENTROPİ tabanlı TOPSIS ve VIKOR yöntemleriyle Bıst-imalat işletmelerinin finansal ve borsa performanslarının karşılaştırılması. Muhasebe ve Vergi Uygulamaları Dergisi, 12 (2), 255-270.

[18] Leong, W.Y.; Wong, K.Y.; Wong, W.P. A New Integrated Multi-Criteria Decision-Making Model for Resilient Supplier Selection. Appl. Syst. Innov. 2022, 5, 8. https://doi.org/10.3390/asi5010008

[19] Göncü, K. K., & Çetin, O. (2022). A Decision Model for Supplier Selection Criteria in Healthcare Enterprises with Dematel ANP Method. Sustainability, 14(21), 13912..

[20] Singh, A., Gupta, A., & Mehra, A. (2020). Best criteria selection based PROMETHEE II method. OPSEARCH (58), 160–180. doi:10.1007/s12597-020-00464-7.

[21] Özdemir, A. (2010). Ürün grupları temelinde tedarikçi seçim probleminin ele alınması ve analitik hiyerarşi süreci ile çözümlenmesi. Afyon Kocatepe Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, 12(1), 55 - 84.

[22] Kabadayi, N., & Sündüs, D. A. Ğ. (2017). Bulanik Dematel Ve Bulanik Promethee Yöntemleri İle Kablo Üretiminde Makine Seçimi. Karadeniz Teknik Üniversitesi Sosyal Bilimler Enstitüsü Sosyal Bilimler Dergisi, 7(14), 239-260.

[23] Eleren, A., & Ersoy, M. (2007). Evaluation of marble extraction methods by using fuzzy topics method. The Journal of the Chamber of Mining Engineers of Turkey, 46(3), 9-22.

[24] Sahin, B., Yip, T. L., Tseng, P. H., Kabak, M., & Soylu, A. (2020). An application of a fuzzy TOPSIS multi-criteria decision analysis algorithm for dry bulk carrier selection. Information, 11(5), 251.

[25] Akpınar, M. E. (2021). An Applıcatıon On The Most Suıtable Supplıer Selectıon Wıth Fuzzy Topsıs And Fuzzy Vıkor Methods. Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, 23(2), 627-640.

[26] Huang, C. Y., Shyu, J. Z., & Tzeng, G. H. (2007). Reconfiguring the innovation policy portfolios for Taiwan's SIP Mall industry. Technovation, 27(12), 744-765.

[27] Raut, R. D., Bhasin, H. V., & Kamble, S. (2011, 6). Evaluation of supplier selection criteria by combination of AHP and fuzzy DEMATEL method. International Journal of Business Innovation and Research, 5(4), 359 - 392. doi:10.1504/IJBIR.2011.041056

[28] Chang, D. Y. (1996). Applications of the extent analysis method on fuzzy AHP. European journal of operational research, 95(3), 649-655.

[29] Charnes, A., Cooper, W. W., & Rhodes, E. (1978). Measuring the efficiency of decision making units. European journal of operational research, 2(6), 429-444.

[30] Kuo, R. J., & Lin, Y. J. (2012). Supplier selection using analytic network process and data envelopment analysis. International Journal of Production Research, 50(11), 2852-2863.

[31] Ar, İ. M. , Gökşen, H. & Tuncer, M. A. (2015). Using Integrated DEMATEL-ANP-VIKOR Method for Supplier Selection in Cable Sector. Ege Academic Review, 15 (2), 285-300. Retrieved from https://dergipark.org.tr/tr/pub/eab/issue/39938/474510.

[32] Opricovic, S., & Tzeng, G.-H. (2004). Compromise solution by MCDM methods: A comparative analysis of VIKOR and TOPSIS. European Journal of Operational Research, 156(2), 445-455. doi:10.1016/S0377-2217(03)00020-1

[33] Dalkey, N., & Helmer, O. (1963). An experimental application of the Delphi method to the use of experts. Management science, 9(3), 458-467.

[34] Gidiagba, J., Tartibu, L., & Okwu, M. (2023). Sustainable supplier selection in the oil and gas industry: An integrated multi-criteria decision making approach. Procedia Computer Science, 217, 1243-1255.

[35] Pearson, K. (1901). LIII. On lines and planes of closest fit to systems of points in space. The London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science, 2(11), 559-572. doi:10.1080/14786440109462720.

[36] Hotelling, H. (1933). Analysis of a complex of statistical variables into principal components. Journal of Educational Psychology (24), 417–441, and 498–520.

[37] Petroni, A., & Braglia, M. (2000). Vendor Selection Using Principal Component Analysis. The Journal of Supply Chain Management, 2(36), 63-69.

[38] To, S., & Kritchanchai, D. Sustainable Supplier Selection in a Hospital Using the Fuzzy TOPSIS method: a Case Study. . roceedings of the 5 th European International Conference on Industrial Engineering and Operations Management, Rome, Italy, July 26-28, 2022

[39] Organ, A. (2013). Bulanık Dematel yöntemiyle makine seçimini etkileyen kriterlerin değerlendirilmesi. Çukurova Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, 22(1), 157-172

[40] Karaoğlan, S., & Şahin, S. (2016). DEMATEL ve AHP yöntemleri ile işletmelerin satın alma problemine bütünleşik bir yaklaşım, DSLR kamera örneği. İşletme Araştırmaları Dergisi, 8(2), 359-375.

[41] Baykasoğlu, A., Kaplanoğlu, V., Durmuşoğlu, Z. D., & Şahin, C. (2013). Integrating fuzzy DEMATEL and fuzzy hierarchical TOPSIS methods for truck selection. Expert Systems with Applications, 40(3), 899-907.

[42] Dalalah, D., Hayajneh, M., & Batieha, F. (2011). A fuzzy multi-criteria decision making model for supplier selection. Expert Systems with Applications, 38(7), 8384-8391

[43] Chen, T. Y., & Tsao, Y. C. (2008). The interval-valued fuzzy TOPSIS method and experimental analysis. Fuzzy Sets Systems, 159, 1410-1428.

[44] Wang, Y. (2018). Application of TOPSIS and AHP in the Multi-Objective Decision-Making Problems. MATEC Web of Conferences, 228, p. 05002.

Journal of Emerging Computer Technologies
Review Article
Received: *2022-08-05* | ***Reviewing:*** *2022-08-06* & *2023-02-27*| ***Accepted:*** *2023-02-27* | ***Online:*** *2023-02-27* | ***Issue Date:*** *2022-12-31*

A Review about Forensic Informatics and Tools

Çiğdem BAKIR
Kütahya Dumlupınar University
Software Engineering Department
Kütahya, Turkiye
cigdem.bakir@dpu.edu.tr
0000-0001-8482-2412

Mecit YÜZKAT
Yildiz Technical University
Computer Engineering Deparment
İstanbul, Turkiye
myuzkat@yildiz.edu.tr
0000-0003-4808-5181

***Abstract*— Due to the rapid increase in the use of internet and electronic devices in our age, forensic informatics is becoming a very important field. A good understanding of forensic processes is necessary for the protection of states, institutions and personal information. In addition, when a crime is committed, it is a great precaution to make the right decision when making decisions about this crime. In the article study, researches on the importance of forensic science, its areas of use and the tools used in these areas were made. The study consists of three main stages. In the first stage of the study, the general definition of forensics, its precautions, common areas of use and recent studies on forensics were examined in detail. networks are offered. In the second stage, the process of collecting, analyzing and reporting, which is a process of forensic informatics, was made and the types of evidence were mentioned. In the third part of the study, information about legal informatics law is given. In the final stages of the conclusion and suggestion section, suggestions were made about the importance of forensic science, the lack of academic understanding of forensic sciences in our country and how these deficiencies can be eliminated.**

Keywords*— *Forensic computing, hardware tools, software tools, mobile forensic computing, cloud computing

I. INTRODUCTION

In today's world, with the spread of electronic devices, a large number of digital forensics crimes are being faced with every passing day. In order to cope with these crimes, it is necessary to know well the new methods of investigation. Thus, before working in the field of digital forensics, it is also necessary to know the steps of the digital forensics process well and to obtain the evidence used in this field without any problems. When incorrect methods are applied to the evidence, the evidence may be damaged, and irreparable consequences may occur.

In the second part of this study, researches made in recent years about forensics were discussed, in the third part, forensic computing (definition of forensics, its current importance and usage areas) were discussed. In the last part of the study, the conclusion obtained with forensic informatics and discussion in detail.

II. LITERATURE REVIEW

In recent years, there has been an increase in studies related to digital forensics, and the importance of this issue is increasing every day. The information obtained in some previous studies related to the issue of digital forensics is briefly mentioned below. In Table 1, studies related to forensic informatics in the literature are given in detail.

TABLE I. CURRENT STUDIES IN THE LITERATURE

Source	Method
Robbins [1]	Judd Robbins, a digital forensics expert, revealed that digital forensics was based on analysis techniques applicable to investigation and legal evidence [1].
Hand and Lin [2]	Hand, Lin, and their colleagues mentioned Bin-Carver, which was the first system of its kind for automatically recovering deleted or corrupted metadata and executable files. In the study conducted with thousands of binary code files, accurate results were obtained with a recovery rate of 93.1% without files being corrupted [2].
Narayanan and Ashik [3]	In their study, Narayanan and Ashik discussed digital forensics analysis tools and their usage in an application. In this study, basic research concepts and how to use a specific tool were explained for beginners in the field of digital forensics [3].
Pal and Memon [4]	In a study conducted in 2009, Pal and Memon touched on file carving (that is, works such as restoring deleted files or recovering data on a corrupted device). While the study was successful in recovering text and images, the same success could not be achieved for video, audio, executable, and other file formats. Therefore, they talked about the creation of new techniques [4].
Ballenthin [5]	It isconducted a study on commercial open source tools, and mentioned the index structure and the contents of index entries. For example; EnCase, FTK and TSK etc. they have recently released INDXParser.py, an open source tool that parses NTFS index files into Excel and CSV file formats, as well as a search for free fields [5].
Mutawa and Baggili [6]	It is focused on conducting forensic analyses in three social networking applications (Facebook, Twitter, and MySpace) that are commonly used on smartphones. The tests were conducted on three popular smartphones (BlackBerry, iPhone and Android). The tests were carried out in the form of installing social networking applications on each device, conducting common user activities through each application, obtaining a forensically healthy image of each device, and performing manual forensic analysis on each resulting image. The results showed that no traces were found in BlackBerry devices, while a significant amount of data that can be recovered and used by forensic investigators was obtained from iPhone and Android phones [6].
Krishnun [7]	In another study, it was mentioned different approaches for digital forensics investigations of flash drives. Three different data collection methods were discussed for creating complete memory copies of flash memory devices. While doing this, 45 different brands and models of USB flash drives were used. Which steps were needed to convert the extracted data in an understandable form by the common forensic media analysis tools was shown. However, it was emphasized that further research was necessary for flash memory data that could not be converted directly to the file system level [7].
Arthur and Venter [8]	In the study, the common points of digital forensics tools and their main differences were discussed, and what features should be developed in these tools to make them achieve effective results on storage devices was mentioned. In addition, some digital forensics tools were used in this study and the authors focused on the missing features of these tools [8].

Source	Method
Guo, Jin, and Shang [9]	In their studies, it was presented the definition and various models of cloud computing. In addition, they compared classic forensic investigations with forensic investigations in the cloud and analyzed the challenges of forensic investigation in cloud environments. For this reason, the necessity of a broader range of technical knowledge on a wide variety of hardware platforms and operating systems, as well as a deep understanding of a wide variety of technologies, applications, networks, has been mentioned with forensics [9].
Van Houten et al [10]	In a study conducted by Van Houten et al., the difficulty of identifying the video source from low-quality videos was deeply examined [10].
Garfinkel [11]	Garfinkel mentioned the design and use of DFXML. As discussed in this study, digital forensics XML (DFXML) is an XML language that allows the exchange of structured forensic information. In digital forensics, DFXML represents the origin of data. DFXML also documents the specific tools used to produce the results and their processing techniques. The automatic reprocessing of forensic information when tools were developed was also discussed in this study [11].
Tang [12]	In another study, the current state of digital forensics investigations, their future trends, and a typical platform of the software system commonly used in Linux were mentioned. In addition, the problems caused by the fact that many of the current works were based on manual applications were discussed [12].
Milani et.al. [13]	Milani et.al. presented an overview of current video processing techniques. They also mentioned the possibility of identifying all possible terms that could be operated on a single signal and footprints that could reveal important information about its origin and use. They showed that this was possible on the assumption that each processing step does not create an excessive amount of distortion on the signal. It did not give good results as a serious deterioration in signal quality would render it useless [13].
Yin Pan et al [14]	Yin Pan et al. conducted a study on games related to digital forensics. They focused on designing and developing game-based digital forensics work in a real computing environment by using the game-based learning (GBL) approach. In this study, interactive visualization was used to help students understand intangible and inaccessible abstract concepts such as deleted, hidden, over-written, or encrypted digital evidence [14].
Yinghua [15]	Yinghua, Slay, and Beckett focused on the topic of verification and validation of tools used in digital forensics. Thus, they conducted some tests and applied these tests to some real tools such as EnCase and FTK, which are widely used in the market. In addition, they mentioned a quantitative model for evaluating the results of verification and validation. In this study, how to evaluate whether a tool was validated was also discussed [15].
Cho [16]	In the study conducted by Gyu Sang Cho, a digital forensics analysis method for a directory on the NTFS file system was presented. In the study, especially if there are a large number of files in the directory, digital forensics methods were used. From a digital forensics perspective, information was provided about how the directory entries and traces on the directory entry record remain when the files are deleted [16].
[17,18]	In this study, fuzzy logic and genetic algorithms were used for intrusion detection systems on server computers. First of all, abnormal behaviors were detected by examining user behaviors over log records [17, 18].
Kobayashi [19]	In their study, Kobayashi and colleagues aimed to detect suspicious areas in a video recorded from a static scene by using noise characteristics to detect changes made on cameras [19].
[21]	Data recovery technology on a computer is one of the most important technologies in the field of digital forensics. Data can be recovered using professional digital forensics tools such as Encase [20] and Easy recovery [21], even in cases where the data has been completely deleted on a computer and even the disk has been formatted more than once.
[22]	Considering the spread of cybercrimes on portable devices, Joe Grand introduced some software for digital forensics works on portable devices with operating systems [22].
Ronghua Shi et al [25]	Ronghua Shi et al. discussed their studies on the design of a matrix-based visualization system for digital forensics in network traffic. They stated that because users' information on the network could be easily obtained from the interface, this system could provide a comprehensive analysis of network traffic and it had certain advantages for efficiently revealing clues related to digital forensics [23].
[24,25]	Forensic network traffic tools, such as TCPDump [24] and Snort [25], capture network traffic in different formats at different levels and analyze them by matching rules and creating event logs.
Ghafarian [26]	In his research, Ahmad Ghafarian focused on the analysis of cloud storage services in digital forensics and he carried out his study on a copy of Dropbox. He analyzed the traffic log files by using the Wireshark forensic network tool. In this way, much more information such as the suspect's file access history, the identity of the person who accessed the file, and the operations performed on the file, was revealed [26].
Khan et al. [27]	Khan et al. compared the conventional network forensics and SDN (Software-Defined Networking) forensics to highlight the fundamental differences between them. They presented a brief motivation for SDN forensics in order to emphasize its significance. Moreover, they discussed challenges faced in SDN forensics by highlighting potential research areas for academicians, researchers, and investigators [27].
Easwaramoorthy et al [28]	Easwaramoorthy et al. used Microsoft One Drive and Amazon Cloud Drive, which are two popular open cloud service providers, to carry out forensic evidence collection procedures through the browser and service provider on a Windows 7 computer [28].
Quick [29,30]	In their research, Darren Quick and his colleagues focused on the collection of data related to users in multiple cloud storage, which is one of the main difficulties in cloud storage [29]. They obtained various types of evidence data that are located on the end-user machine in cloud storage and are access points of forensic investigators for examining and collecting evidence in the time period [30].

III. FORENSIC COMPUTING

Digital forensics is also described as the process of examining electronic devices for the purpose of collecting evidence related to a crime on all types of electronic devices by using special examination and analysis techniques [31].

James Barek likens forensic informatics to the process of examining the crime scene or performing an autopsy on a victim. The purpose of digital forensics can be defined as the collection, examination, analysis, and reporting of evidence, respectively [32].

Nowadays, the potential for harm caused by an ever-increasing number of digital forensics crimes due to the widespread use of electronic devices continues to enter and occupy our lives. The Federal Bureau of Investigation (FBI) estimates that the cost of cybercrime in the world is more than 100 billion dollars a year. In order to cope with these crimes, it is necessary to know well the new and previous methods of investigation. Due to improper intervention, evidence can be damaged, destroyed, or changed [33].

Digital forensics investigation techniques help to solve cases related to not only the crimes, such as cyber hacking or child pornography, but also other crimes such as murder, terrorism, organized crime, tax evasion, drug trafficking, and extortion. In the digital age in which we live, it is practically not possible to obtain the types of evidence needed to solve many of the cases brought into the court system. Therefore, nowadays, digital forensic science is an extremely reliable and useful resource that is necessary for many cases.

Modern digital forensics has a wide range of applications. With the rapid development of informatics in the world, digital forensic science is also developing in parallel, and new ones are being added to its application areas every day. Common application areas are given below:

- Storage and recovery of data
- Conversion of data safely
- Transportation of data safely
- Encryption and decryption
- Detecting and preventing abuses
- Search for hidden files
- Control works in financial audits
- Investigation and analysis of all types of commercial disputes
- Reviews related to legal proceedings and trials

In the literature, Digital Forensics is divided into different types with very different names. In fact, although they are divided into different types, the functioning of the processes in each branch of digital forensics is the same. Within the scope of this study, we examine the types of digital forensics as four different sub-branches in general: Computer Forensics, Network Forensics, Mobile Forensics, and Social Network Forensics.

Nowadays, forensic investigations performed on computers and their components are known as the most commonly used digital forensics type. In the field of computer forensic science (computer forensics), it is necessary to ensure the safety and examination of all types of computers and their components, used by the offender or located in the environment where the crime was committed, by the forensic units in accordance with the rules of procedure [34].

One of the issues that should be considered at the first stage for all types of computers and their components found at the crime scene is to take the "Write Blocker" precaution. That is, first of all, it is necessary to take images of computer components that are at the crime scene.

Network Forensics refers to the forensic examination carried out as a result of criminals infiltrating the network systems of any institution or persons and damaging these systems for financial gain or personal entertainment, as well as monitoring carried out by forensic units to prevent or detect such incidents. In such cases, it is necessary to examine the packets outgoing over the network when performing network forensic analysis. The most important evidence that can be analyzed is packet data captured over the network.

Thanks to network forensics, transmitted packets are examined instantaneously or at certain time intervals. The important data obtained as a result of the examinations are used in early warning systems when it is considered necessary.

Network forensics is usually used in two conditions. The first is related to security. This includes monitoring a network for abnormal traffic and identifying interventions. For example, suppose that through a network, the security mechanism has been breached, and after obtaining important information on a computer, all log files have been deleted. In this case, only network-based data and signs can be used as evidence [35]. The second case is more related to law enforcement agencies. This may include tasks such as analyzing network traffic, reassembling transferred files, and ensuring the security of communications.

Mobile Forensics (or mobile device forensics) is the acquisition of criminal devices for all types of crimes committed using different brands of mobile devices, the identification, analysis, and reporting of information that may be a criminal element in such devices by using the necessary software, and transmission of them to the judicial authorities. The term mobile device usually refers to mobile phones; however, it may also refer to any digital device with both internal memory and communication capabilities, including PDA devices, GPS devices, and tablet computers.

Mobile devices can be used to save various personal information, such as photos, calendars, notes, and SMS/MMS messages. Smartphones can also contain video, email, web browsing information, location information, social sharing messages, and contacts.

The important reasons why mobile devices have been used a lot in digital forensics in recent years are as follows [36]:

- The fact that they store personal and corporate information
- Increased use of mobile phones for communication
- The use of mobile phones in online transactions
- The fact that many of the recent crimes have been committed using mobile phone devices

The biggest disadvantage encountered when conducting a digital forensics investigation on mobile devices is that because many different brands and models of smartphones are used today, the investigations to be conducted are model-dependent in some cases.

Social Network Forensics has been accepted as a new type of digital forensics in recent years due to the increasing number of social networking sites in parallel with the spread of the internet and, accordingly, the increasing number of criminal acts [37]. Due to the widespread use of social networking sites, the spread of malware has become easier and some acts such as human trafficking, drugs, prostitution, and fraud have increased. At the stage of detecting these actions and evaluating electronic evidence, social network forensics is used.

Important social networking applications such as Facebook, Twitter, and Linkedin can cause misuses such as copyright infringement, data protection violations, libel,

identity theft, harassment, and the dissemination of confidential information. The means used to prove an incident that has occurred are called evidence [38]. Digital forensic evidence is all types of information or digital objects that can record data and perform all kinds of automated operations on this data and that can be accepted at the stage of clarification of a committed crime.

Based on the above description, it can be said that all digital devices that have the ability to store data during the intervention at the initial stage of the incident are potential evidence and must be examined. Any information and data that can be transmitted or stored by digital devices are called digital evidence.

When digital forensics evidence is compared with classical evidence, it can be said that they are much more sensitive than classical evidence. This is because it is very difficult to notice by looking from the outside when changes are made to digital forensics evidence. However, the changes made to the classical evidence can be noticed very easily [39]. Digital forensics evidence should have all the characteristics such as acceptability, reality, integrity, and reliability that should be present in classical evidence.

Nowadays, due to the rapid development of technology, new types of forensic evidence are emerging every day. Some of the most important types of digital forensics evidence are as follows:

- Computers systems (desktop, laptop, server) and their data files
- Computer system components (HDD, Memory) and their data files
- Memory cards, external hard drives and removable backup tools
- Digital cameras and their data
- Mobile devices and their data
- Network devices and their data
- Printers, scanners, and their data
- Biometric tools and their data
- All types of credit cards and their data
- Electronic watches and their data

Digital forensics investigations usually follow the standard stages of the forensic process. To understand and address the legal framework of digital forensics evidence, the stages of the process model are shown in Fig 1. These stages are evidence acquisition, examination, analysis, and reporting.

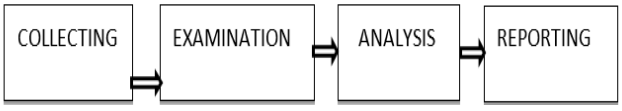


FIG I. FORENSIC COMPUTING PROCESSES

When an accident, crime, or any bad event occurs, the need for an investigation arises. The origins and causes of the incident can be investigated with the help of digital media [40, 41].

It is clear that digital media is useful in investigating the roots and causes of a crime. As already mentioned, most of the crimes have digital links in some way. The digital forensics investigation is a difficult process; evidence may be lost due to reasons such as incorrect shutdown of the system, manipulation or modification of digital evidence, and access to evidence several times [42]. Therefore, finding digital evidence to combat a crime is a reliable, popular, and effective measure. Since digital evidence helps to explain the sequence of the crime [43, 44], it also helps to catch the criminal.

When conducting a digital forensics investigation, many options and techniques can be used to obtain evidence from the environment in which the crime has been committed. Digital forensics investigation teams have certain authorities to collect evidence from the criminal environment [45, 46]. Digital evidence can be obtained from various sources such as mobile phones, digital cameras, pen drives, hard drives, and memory devices. Special attention should be paid to digital evidence since they are vulnerable to interference or can be destroyed.

In addition, log files containing very important information such as remote access, date, time, who is connected to the computer, and who is using it when the connection is lost can also be a great source of evidence. Collecting evidence and catching a criminal who has committed a crime on flash memory or the internet are equally difficult. This is due to the fact that the tools that can be used to collect evidence are either of poor quality or are not sufficient in terms of revealing the identity of the criminal [47].

After the evidence acquisition stage, the obtained data is processed. Each part of the evidence is matched to form the whole event sequence and to reshape the crime scene [48, 49]. Before proceeding to the examination process, investigation methods related to the committed crime should be determined and an examination plan should be put forward. The purpose of the examination plan is to find out what types of data related to crime should be investigated. At this stage, relevant information is identified and extracted from the collected data using appropriate tools and techniques by experts. In the world, software such as EnCase, FTK, and X-Wasy, which are digital evidence examination software accepted by international standards, are often used by digital forensics authorities [50].

The analysis, which is the third stage in the digital forensics process, is the stage where the necessary technical analyzes are performed on the evidence. When the data obtained at this stage were compared with the original data, there should be integrity and content verification between the evidence. The purpose of the analysis is to put forth the correct data revealing the crime as evidence and to make it ready for the reporting stage in a good way.

In the reporting, which is the final stage of digital forensics, the evidence obtained and analyzed must be reported in an explanatory and understandable language for use by the judicial authorities. In relation to the report to be prepared, the following issues should be considered.

- The report must be being completed.
- The report should also be understandable for people without technical knowledge.
- There should be concrete information in the report.
- The digital forensics methods used in the report should be explained in detail.
- In the report, it should be proved that the integrity of the evidence is not destroyed.
- The report should help to uncover the crime and catch the criminal.

IV. Conclusion And Discussion

Due to the widespread use of information technologies in our country, as in the whole world, it also brings security problems. It is not enough to fight cyber crimes committed through information technologies only with law enforcement. In the fight against cyber crimes, both forensic laboratories and expert personnel are needed.

The principle of protection of personal data and the right to privacy, which are important issues to be considered during the collection of electronic evidence in international law, have also been regulated and secured. The United Nations (UN) Universal Declaration of Human Rights, especially article 12, and article 17 of the UN International Covenant on Civil and Political Rights, in the UN's policy decisions on the protection of personal data issued on various dates, the OECD at different times. The privacy of private life and the protection of personal data are guaranteed in its decisions and many other international texts [51].

Forensic software generally includes many functions, but some tools come to the fore for certain functions [52, 53]. These functions can be grouped as e-mail review, message review, internet history review, data acquisition and location information acquisition. We can group forensic tools according to certain characteristics. As we can group hardware-based and software-based, it can be grouped in various ways according to whether it is open source or not, and finally, according to its functions. In this study, we divided the forensic tools into two as hardware and software tools.

Before doing research, a forensic expert should have a good knowledge of the internal and external structure of the system and the settings of the hard disks. Today, there are many forensic hardware tools such as FRED, Image MASSter Solo, Tableau from the field of forensics. Each hardware tool has different functions according to the research scenario. In addition, these tools include necessary write blockers to prevent tampering with evidence [54].

Today, new forensic software is constantly being developed. The software tools used in this field often vary according to the type of investigation being performed. Forensic software tools can be characterized by data recovery tools, partition tools, disk colonization tools, recovery tools, test tools, RAM test utility, system speed test, hard disk tools, system information tools, DOS tools, and other tools.

Encase, ftk, X-ways are the most used software in the field of forensic informatics. We cannot reach definite conclusions about which of these softwares are better because each software is better in a certain area. For example, while indexing and search methods are more advanced in ftk software, this feature may not be available in all versions of other software. In addition, while the scripts used in Encase software are frequently used by users, this is not the case in other software. Apart from these, it is more logical for a forensic software user to choose which software is more comfortable to use [55].

Digital forensics science is a discipline that is changing and developing every day. Individuals, institutions, or states engaged in scientific studies in this field should adapt to innovations in a short time. Today, with using digital devices by many people, cybercrime is also increasing day by day; in parallel, the analysis of digital evidence is becoming an important element at many crime scenes. The principle of personal data protection and ensuring the confidentiality of private life take place among the important issues to be considered during the collection of evidence in digital forensics investigations. To be able to cope with these crimes, the new and previous methods of investigation should be known well. Due to improper intervention, evidence can be damaged, destroyed, or changed. Digital forensics investigations techniques help not only to solve cybercrime, such as hacking or child pornography, but also to solve other crimes, such as murder, terrorism, organized crime, tax evasion, drug trafficking, and extortion. In the digital age in which we live today, it is practically impossible to obtain the types of evidence needed to solve many of the cases brought into the court system. Although digital forensics has been an exciting popular profession that pays attention to the human element in recent years, it also contains various difficulties due to the need to uncover digital evidence in an ever-changing environment. Due to technological advances and situations where anti-forensics methods can easily come into play, experts working in this field need to comply with current standards and constantly review standard stages of work.

Within the scope of this study, national and international books, theses, articles, papers published in recent years related to digital forensics and internet sites that are good in this field were examined in detail. In the first part of this research, the literature studies conducted in recent years related to digital forensics were included generally. In the literature review, digital forensics tools and methods used to automatically recover deleted or corrupted metadata and files by using different methods were mentioned, and a comparison of these methods was made. In the second part of the research, the general definitions used in the digital forensics literature were mentioned, and taking into account the fact that in today's world the cost of cybercrime is more than 100 billion dollars a year, the importance of digital forensics was discussed. In addition, the application areas of digital forensics were briefly mentioned. In terms of the types of digital forensics, computer, network, mobile, and social network forensics sciences were touched upon in general terms. While studying the digital forensics processes, the standard stages of the forensic process and the evidence acquisition, examination, analysis, and reporting stages were discussed in detail, and the

legislation of digital forensics was touched on shortly. In addition, the general characteristics of hardware and software tools used in digital forensics investigations were mentioned in detail. A comparison of the most popular of these tools was made. This research was prepared as a preliminary study on what kind of path should be followed when conducting a study on digital forensics. Although there are studies related to digital forensics conducted by private companies in our country, any study at the doctoral dissertation level has not been conducted in this field in academic terms. In this context, it is believed that both the provision of high-quality undergraduate education related to digital forensics and the organization of good certificate programs related to this issue will make a positive contribution to this field in our country.

REFERENCES

[1] Walker, C. (2006). Computer forensics: bringing the evidence to court. Retrieved August, 23, 2008.

[2] Hand, Scott, et al. "Bin-Carver: Automatic recovery of binary executable files." Digital Investigation 9 (2012): S108-S117.

[3] Narayanan, A. Sankara, and M. Mohamed Ashik. "Computer Forensic First Responder Tools." Advances in Mobile Network, Communication and its Applications (MNCAPPS), 2012 International Conference on. IEEE, 2012.

[4] Pal, Anandabrata, and Nasir Memon. "The evolution of file carving." IEEE Signal Processing Magazine 26.2 (2009): 59-71.

[5] William Ballenthin, "NTFS INDX Attribute Parsing", http://www.williballenthin.com/forensics/indx/index.html. [Accessed: 10-May-2021]

[6] Al Mutawa, Noora, Ibrahim Baggili, and Andrew Marrington. "Forensic analysis of social networking applications on mobile devices." Digital Investigation 9 (2012): S24-S33.

[7] A forensics overview and analysis of USB flash memory devices, Krishnun Sansurooah. Proceedings of the 7th Australian Digital Forensics Conference, Edith Cowan University, Perth Western Australia,2009.

[8] Arthur, Kweku K., and Hein S. Venter. "An Investigation Into Computer Forensic Tools." ISSA. 2004.

[9] Guo, Hong, Bo Jin, and Ting Shang. "Forensic investigations in cloud environments." Computer Science and Information Processing (CSIP), 2012 International Conference on. IEEE, 2012.

[10] Wiger van Houten, Zeno J. M. H. Geradts, Katrin Franke, and Cor J. Veenman, "Verification of video source camera competition (camcom 2010)," in ICPR Contests, 2010.

[11] Garfinkel, Simson. "Digital forensics XML and the DFXML toolset." Digital Investigation 8.3 (2012): 161-174.

[12] Ling, Tang. "The study of computer forensics on linux." Computational and Information Sciences (ICCIS), 2013 Fifth International Conference on. IEEE, 2013.

[13] Bestagini, Paolo, et al. "An overview on video forensics." Signal Processing Conference (EUSIPCO), 2012 Proceedings of the 20th European. IEEE, 2012.

[14] Pan, Yin, et al. "Game-based forensics course for first year students." Proceedings of the 13th annual conference on Information technology education. ACM, 2012.

[15] Guo, Yinghua, Jill Slay, and Jason Beckett. "Validation and verification of computer forensic software tools—Searching Function." digital investigation 6 (2009): S12-S22.

[16] Cho, Gyu-Sang. "NTFS Directory Index Analysis for Computer Forensics." Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2015 9th International Conference on. IEEE, 2015.

[17] Kaur, Harjinder, and Nivit Gill. "Host based anomaly detection using fuzzy genetic approach (FGA)." International Journal of Computer Applications 74.20 (2013).

[18] Deepak Scholar, Hitesh Gupta, "Digital Crime Investigation using various Logs and Fuzzy rules: A Review", IJARCCE, Vol 2, Issue 4, April, 2013.

[19] Michihiro Kobayashi, Takahiro Okabe, and Yoichi Sato, "Detecting forgery from static-scene video based on in-consistency in noise level functions," IEEE Transactions on Information Forensics and Security, vol. 5, pp. 883– 892, 2010.

[20] Li Weiwei. Computer Forensics Analysis based on EnCase System. Jilin Normal University Journal. 2011. Vol 32.

[21] Kroll Ontrack. Ontrack EasyRecovery. http://www.krollontrack.co.uk/data-recovery/data-recovery-software/. [Accessed: 6-May-2021]

[22] [Joe Grand. pdd: Memory Imaging and Forensic Analysis of Palm OS Devices. Proceedings of the 14th Annual first Conference on Computer Security Incident Handling and Response. 2002.

[23] [Shi, Ronghua, et al. "A Matrix-Based Visualization System for Network Traffic Forensics." IEEE Systems Journal 10.4 (2016): 1350-1360.

[24] [Shorey, R., Kamra, A., Kapila, S., Khurana, V., & Yadav, V. (2006). U.S. Patent No. 7,065,482. Washington, DC: U.S. Patent and Trademark Office.

[25] [Snort. [Online]. Available: http://www.snort.org [Accessed: 4-May-2021]

[26] Ghafarian, Ahmad. "Foreniscs analysis of cloud computing services." Science and Information Conference (SAI), 2015. IEEE, 2015.

[27] [Khan, Suleman, et al. "Software-Defined Network Forensics: Motivation, Potential Locations, Requirements, and Challenges." IEEE Network 30.6 (2016): 6-13.

[28] Easwaramoorthy, Sathishkumar, et al. "Digital forensic evidence collection of cloud storage data for investigation." Recent Trends in Information Technology (ICRTIT), 2016 International Conference on. IEEE, 2016.

[29] Quick, D., & Choo, K. K. R. (2013). Dropbox analysis: Data remnants on user machines. Digital Investigation, 10(1), 3-18.

[30] Quick, D., & Choo, K. K. R. (2013). Digital droplets: Microsoft SkyDrive forensic data remnants. Future Generation Computer Systems, 29(6), 1378-1394.

[31] Adli bilişim, http://www.leylakeser.org/2008/07/adli-biliim-cmk-md-134-ve-dndrdkleri.html [Accessed: 2-May-2021].

[32] Kim, Y., Kim, K.J.,"A Forensic Model on Deleted-File Verification for Securing Digital Evidence", 978—1-4244-5493-8710 IEEE, 2010;

[33] Ademu, I. O., Imafidon, C. O., & Preston, D. S. (2011). A new approach of digital forensic model for digital forensic investigation. Int. J. Adv. Comput. Sci. Appl, 2(12), 175-178.

[34] Peisert, S., Bishop, M., & Marzullo, K. (2008, May). Computer forensics in forensis. In Systematic Approaches to Digital Forensic Engineering, 2008. SADFE'08. Third International Workshop on (pp. 102-122). IEEE.

[35] Erik Hjelmvik, Passive Network Security Analysis with NetworkMiner http://www.forensicfocus.com/passive-network-security-analysis-networkminer. [Accessed: 5-May-2021]

[36] [Ahmed, R., & Dharaskar, R. V. (2009, March). Mobile forensics: an introduction from Indian law enforcement perspective. In International Conference on Information Systems, Technology and Management (pp. 173-184). Springer, Berlin, Heidelberg.

[37] Özocak, Gürkan, "Sosyal Medyada İşlenen Suç Tipleri ve Suçluların Tespiti", Yenimedya Çalışmaları II. Ulusal Kongresi – Kongre Kitabı, Kocaeli, 2013, s. 465.

[38] Uğur BAHADIR – Devletler Özel Hukukunda İspata Uygulanacak Hukuk http://www.turkhukuksitesi.com/makale_131.htm. [Accessed: 5-May-2021]

[39] Özbek, M. (2013). Adli bilişimde delillerin toplanması ve incelenmesi (Doctoral dissertation, İstanbul Bilgi Üniversitesi).

[40] Bahadur, P., & Yadav, D. S. (2015, November). Computer forensics-digitized science. In SAI Intelligent Systems Conference (IntelliSys), 2015 (pp. 1025-1031). IEEE.

[41] Dunbar, B (January 2001). "A detailed look at Steganographic Techniques and their use in an Open-Systems Environment".

[42] Digital forensics and the legal system: A dilemma of our times James Tetteh Ami-Narh,Patricia A.H. Williams, Proceedings of the 6th Australian Digital Forensics Conference, Edith Cowan University, Perth Western Australia,December, 2008.

[43] Baryamureeba, V., & Tushabe, F. (2004, August). The enhanced digital investigation process model. In Proceedings of the Fourth Digital Forensic Research Workshop (pp. 1-9).

[44] Conference on Digital Forensics, Security and Law, 2006 http://www.digitalforensics-conference.org/CFFTPM/CDFSL-

proceedings2006-CFFTPM.pdf Marcus K. Rogers ,James Goldman, Rick Mislan,et. al.

[45] Various (2009). Eoghan Casey, ed. Handbook of Digital Forensics and Investigation. Academic Press. p. 567. ISBN 0-12-374267-6. Retrieved 27 August 2010.

[46] Geiger, M. (2005, August). Evaluating Commercial Counter-Forensic Tools. In DFRWS.

[47] Remote Access Forensics for VNC and RDP on Windows Platform. Paresh Kerai, Proceedings of the 8th Australian Digital Forensics Conference, Edith Cowan University, Perth Western Australia, November,2010.

[48] Noblett, M. G., Pollitt, M. M., & Presley, L. A. (2000). Recovering and examining computer forensic evidence. Forensic Science Communications, 2(4), 1-13..

[49] Reith, M., Carr, C., & Gunsch, G. (2002). An examination of digital forensic models. International Journal of Digital Evidence, 1(3), 1-12.

[50] Altschaffel, R., Kiltz, S., Dittmann, J., "From the Computer Incident Taxonomy to a Computer Forensic Examination Taxonomy", 2009 Fifth International Conference on IT Security Incident Management and IT Forensics, 2009.

[51] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,OECD,http://www.oecd.org/document [Accessed: 10-May-2021]

[52] Özen, M., & Özocak, G. (2015). Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama ve El Koyma Tedbirinin Hukuki Rejimi (CMK M. 134). Ankara Barosu Dergileri, 73(1).

[53] Adli bilişim, http://www.telepati.com.tr/agustos12/konu8.htm.[Accessed: 5-May-2021].

[54] Bill Nelson, Amelia Phillips, Frank Enfinger, Chris Steuart, Computer Forensics and Investigation, Cengage Learning, 2010 ISBN: 1435498836,9781435498839.

[55] Forensic, httpwww.dijitaldeliller.comyazilimlar.htm. [Accessed: 10-May-2021].