University of Kerbala
College of Computer Science
and Information Technology

Kerbala Journal of Computing and Technology

Available Online

Vol. 1, Issue 0

June 2025

Table of Content

Kerbala Journal of Computing and Technology 2025

Academic Awareness Dictionary of Cyber Security

Meeras Salman Al-Shemarry[a],Elham Mohammed Thabit Alsaadi[a] ,

Maha Sabri Altememe[a], Azhar Ali Abbas[a]

[a]Department of Information Technology, College of Computer Science and Information Technology, University of Kerbala, karbala, Iraq

Received: 17 / 02 /2025
Accepted: 21 / 05 /2025
Published: 30 / 06 / 2025

Keywords:

Search engines, Dictionary application , Cybersecurity concepts , Fontend, Backend

ABSTRACT

The advancement of technology has significantly simplified the process of searching for unfamiliar keywords on Google and other search engines. This development is more effective, but not better. This is due to factors such as device battery consumption, internet connection; time spent searching for a specific term, and others, which become apparent when utilizing search engines. Hence, the development an offline and regularly updateable Android dictionary application is crucial. The main objective of this project is to create an online dictionary to facilitate access to academic terms exclusively for cybersecurity concepts. With the help of dictionaries, students and researchers in particular can better understand their topics, improve their communication, and improve their ideas and information for any subject from other disciplines by understanding the meaning of terms correctly and understandably according to their field of circulation in the academic, governmental or industrial side.

1. Introduction

There is now substantial evidence to support the assertion that technology plays a crucial role in people's lives. In recent years, with the explosive growth in the number of mobile applications, they have become one of the most advanced technologies [1]. Although a considerable number of researches have been done to implement dictionary application for android devices for many purposes to facility many services for society [2-5], little attention has been paid to the use of technology-based such as Android-based application in particular. Therefore, as technology develops [7-8], we need an application that can support and accelerate vocabulary search as a replacement for thick books or dictionaries so that we can carry it anywhere and at any time. The purpose of the current research is to contribute to the design of an offline awareness dictionary of cybersecurity concepts electronically by developing an Android-based dictionary application for smartphones. For students, teachers, and anyone interested around the world, the dictionary plays an important role in many ways. For example, dictionaries can help students better understand their subjects, improve their communication, and expand their ideas and information about any topic by correctly understanding the meaning of words. There are different types of scientific dictionaries have been designed for several purposes. For example, for medical professionals, the dictionary includes medical terms, and for computer

∗**Corresponding author:** Meeras Salman Al-Shemarry

Email address: meeras.s@uokerbala.edu.iq

science, the topic of cybersecurity includes cybersecurity terms. Therefore, there is an urgent need to develop an Android dictionary application.

2. Background and Related Works

Android phones have become an indispensable part of most people's lives [9]-[13]. Digital dictionary applications are one of the applications that are designed to make users' daily lives easier. With digital dictionaries on smartphones, users no longer need to rely on traditional dictionaries that are difficult to carry around[14]. There are many websites that have electronic dictionary features, usually specialized in certain subject areas. However, they do not provide all the features of a dictionary in one place. Electronic dictionaries also consume battery power and the internet cost is high. This study deals with the Android application "Dictionary" application, which can be used on smartphones running the Android operating system. Since it is an offline application, it consumes minimal battery and does not require an internet connection. Through this extend, our fundamental objective is to supply users with the most excellent stage through which they can get to a word reference to find a basic and exceedingly scholarly meaning of cybersecurity concepts in a straightforward and productive way. Highlights incorporate giving implications, equivalent words and antonyms for words and giving cases to assist the client understand the settings. We chose to construct this app as a way for individuals to move forward their lexicon and quality within the concept of cybersecurity.

3. Proposed Model

A cybersecurity glossary application was developed using the waterfall model [15][16]. This template builds on the fact that the template has covered all the development related issues to produce an Android-based English glossary of cybersecurity concepts. The waterfall model steps are (1) Potential and problems; (2) System design needs with data collection; (3) Product design; (4) Implementation and unit testing. The development model for this project is shown in Fig. 1. The goal of this project is to provide users with a dictionary of cybersecurity concepts. The development model for this project is shown in Fig. 1. The goal of this project is to provide users with a dictionary of cybersecurity concepts. They can also find examples to understand cybersecurity concepts. In this application, we provide simple dictionary for cybersecurity concepts as android application.

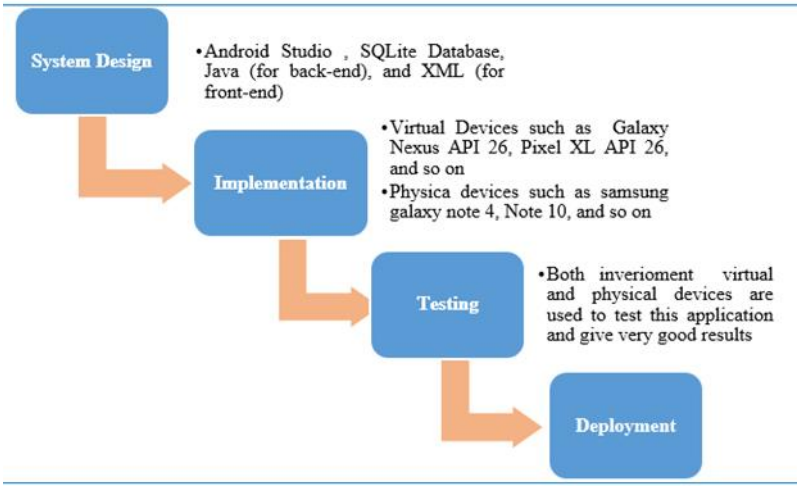


Fig. 1- The Development Model for Cybersecurity Dictionary application

The cybersecurity dictionary consists of 3 core parts: initial view, search view, and display results. Fig. 2 shows the architecture of the project model.

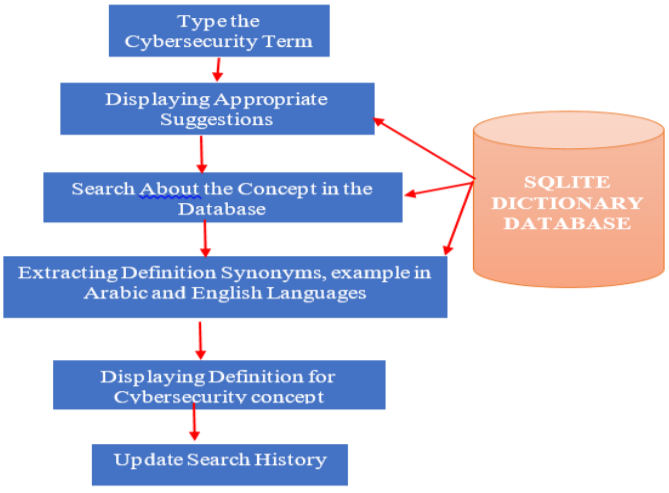


Fig. 2 - Architecture of the project model

3.1. Setup Software

This section describes all software and programming language that used to implement and developed the android word reference application. These incorporates Android Studio, SQLite Database, Java and XML.

3.1.1 The Environment of Android Studio

3.2. Android studio is the official integrated development environment (IDE) for developing Android applications. To back application improvement on the Android working framework, Android studio employments a grade-based construct framework, emulator, code formats, and integration with GitHub. Each extend in Android Studio contains one or more modules with source code and asset records. These modules incorporate Android app modules, library modules, and Google App Motor modules. We utilized Android Studio as an IDE to create this app as shown in Fig 3.

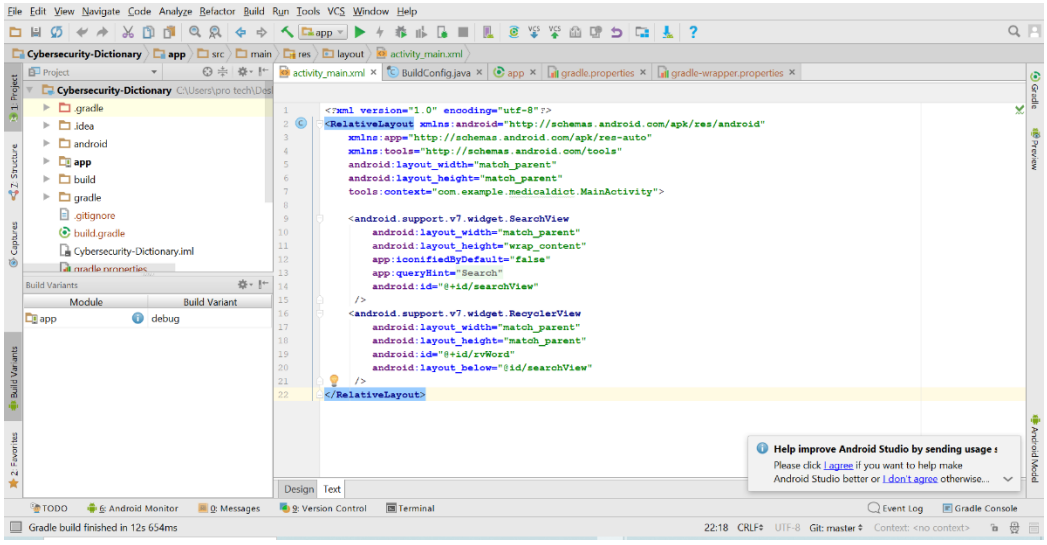


Fig. 3 - The Visual Studio Environment for Android Studio

3.1.2 SQLite Database

SQLite could be a running library that executes an intelligently, standalone, server less, configuration-free SQL database motor. SQLite is the world's most broadly used database and has more applications than ready to tally, counting numerous high-profile ventures. We utilized SQLite (see Fig. 4) to form a cybersecurity word reference database containing hundreds of cyber terms, their definitions, equivalent words, antonyms, and cases in both Arabic and English. The database is associated to this application utilizing Android SQLite libraries with Android Studio as a middleware.

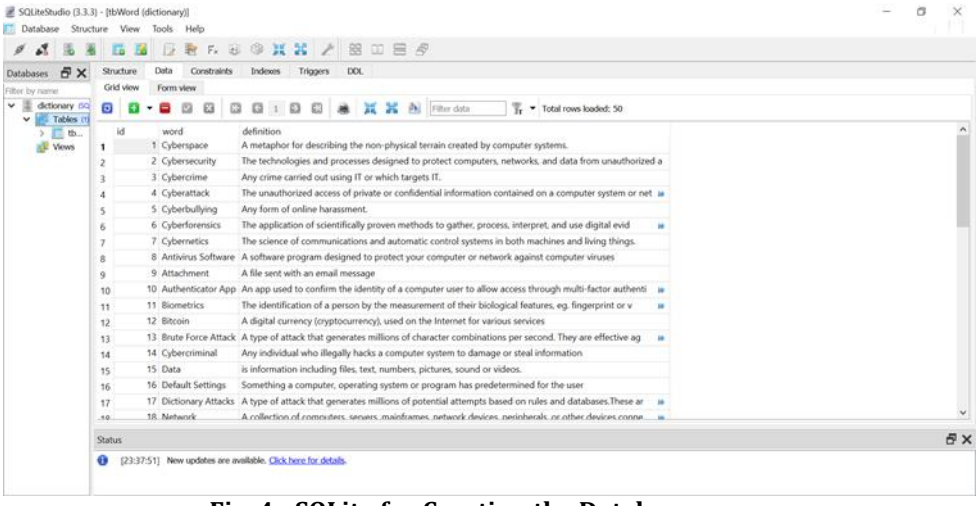


Fig. 4 - SQLite for Creation the Database

3.1.3 Backend Requirements

App include plan permits engineers to make intuitively applications that work consistently. Java is more dynamic than C or C++, because is planned to adjust to an advancing environment (see Fig. 5). Java programs can carry a gigantic sum of runtime data that utilized to confirm and resolve protest gets to amid execution. The most recent adaptation of Java Standard Version is Java SE 8. With the headway and far reaching ubiquity of Java, different setups have been outlined to suit distinctive sorts of stages.

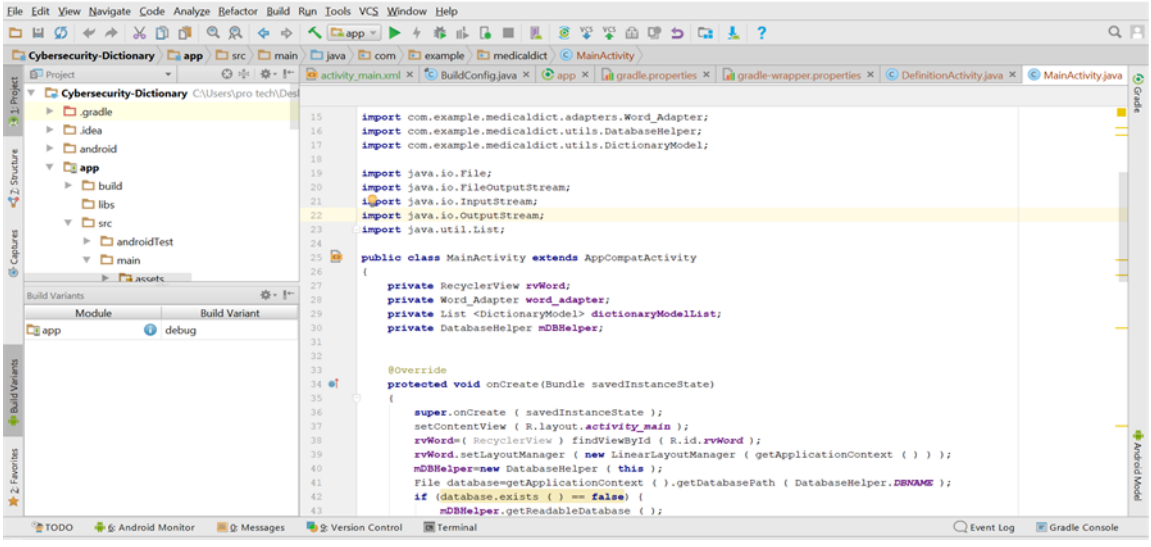


Fig. 5 - Java Programming Code for the Application

3.1.3 Frontend Requirements

XML stands for Extensible Markup language. It could be a content markup inferred from the Standard Generalized Markup language (SGML). XML labels characterize information and are used to store and organize it,

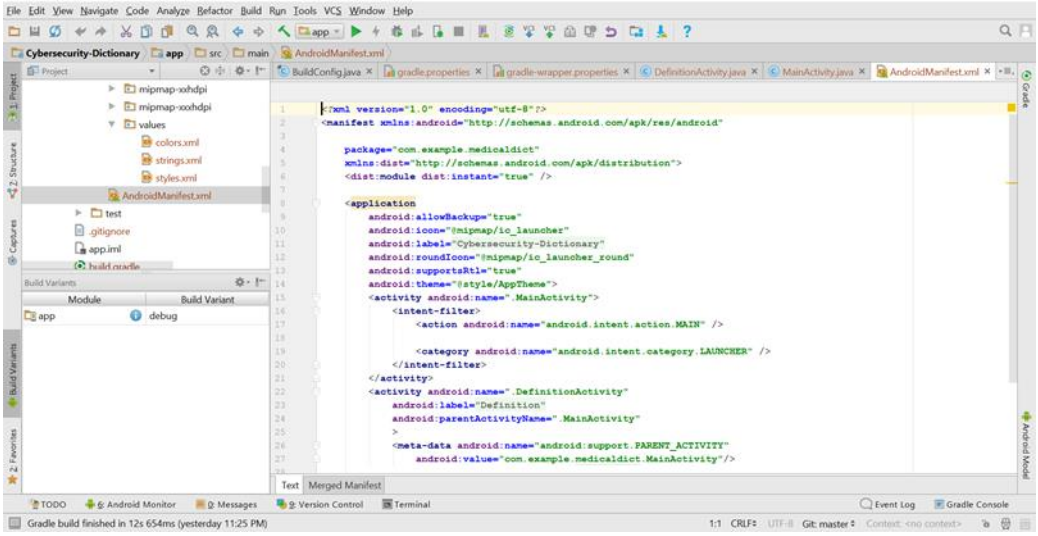


Fig. 6: XML Code for the Application

4. Experimental Results and Discussions

This section displays the output of this study. The test result has been visualized on different features.

4.1 Graphical User Interface

This project has been implemented in two environments: using virtual mobile devices and using real android devices.

4.1.1 Virtual Devices

The cybersecurity dictionary application can implement using many types of virtual android devices (see Fig. 7)

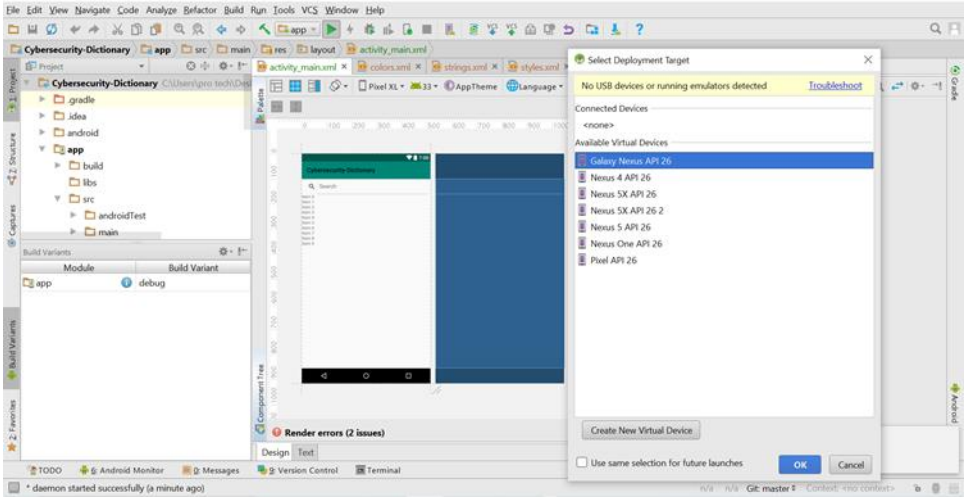


Fig. 7: Run Application Interface Using Virtual Devices

If the required version or model for virtual android device does not found in the list you can create a new virtual device (see Fig. 8) or by download it from internet (see Fig. 9).

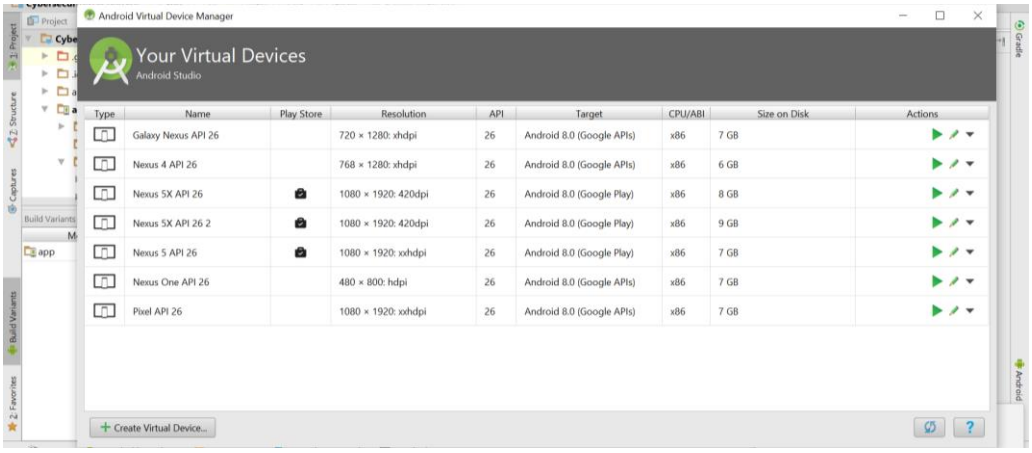


Fig. 8 -Create a New Virtual Device

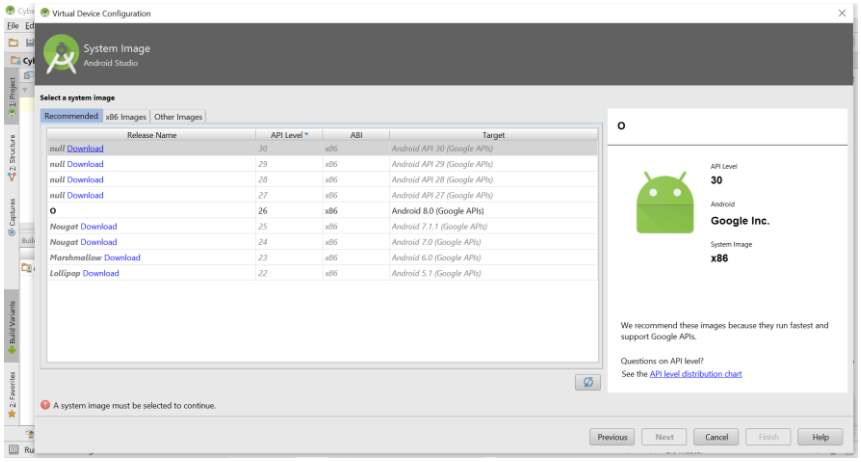


Fig. 9 - Download a New Virtual Device

The default mobile home screen page displayed when the user opens this application for the first time and then the main menu of the cybersecurity dictionary displayed. We selected the Galaxy Nexus API 26 model to implement the cybersecurity dictionary application and the user interface (UI) can be seen in Fig. 10.

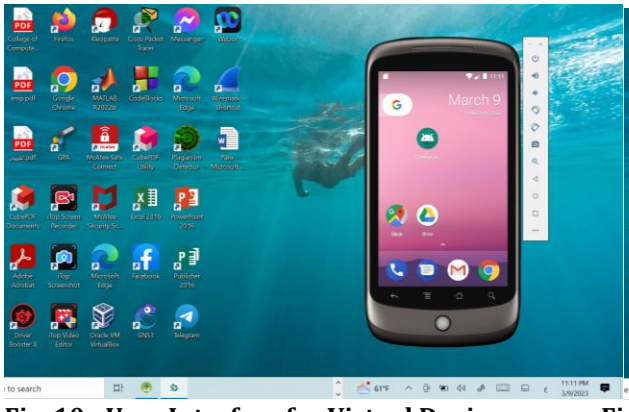


Fig. 10 - User Interface for Virtual Device

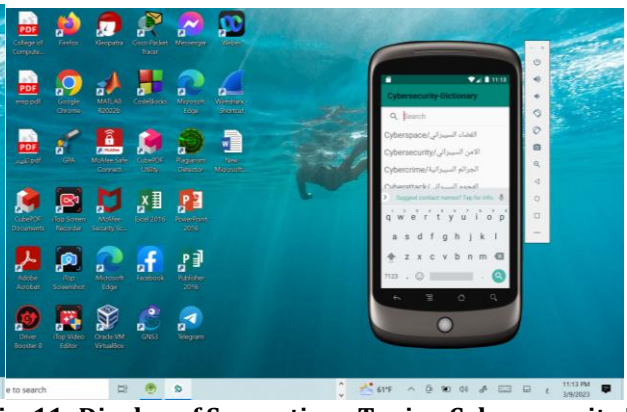


Fig. 11- Display of Suggestions Typing Cybersecurity Term

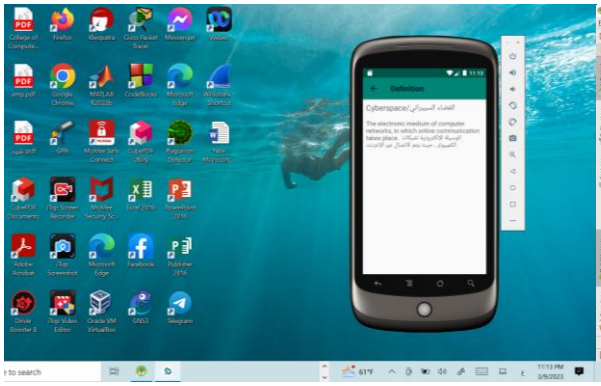


Fig. 12- Definition Option Displayed

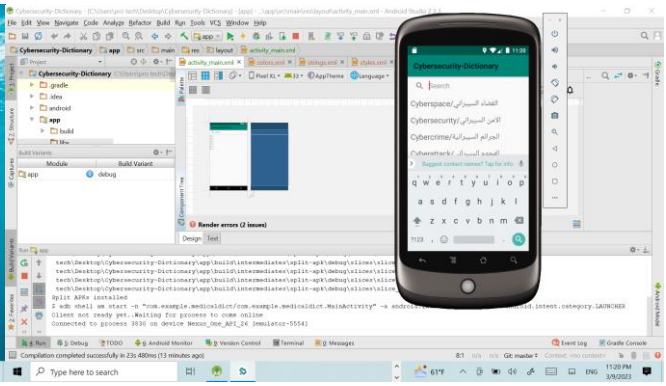


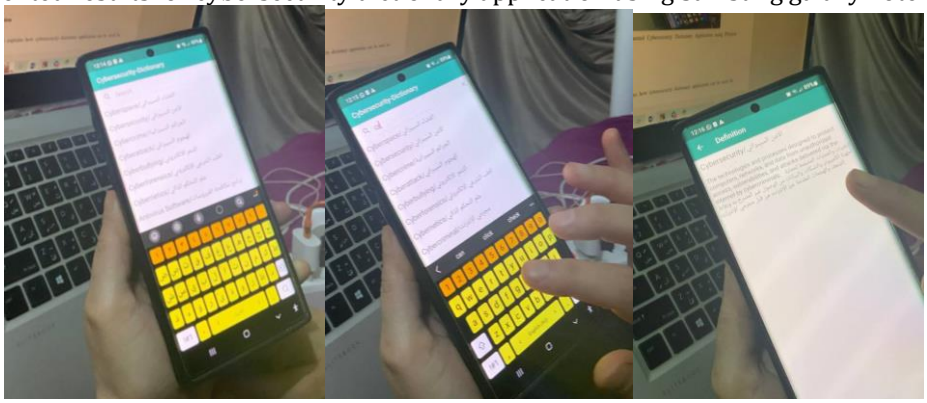
Fig. 13- Main UI of the Application in Android Studio

4.1.2 Physical Devices

This application also implemented on the physical android operating system devices such as Samsung galaxy note 4, 5, 9, and 10. Those are our mobile phone devices we can implement application for any android devices by using USB cable by connect it computer and other side with android mobile. After that doing run for application and select the physical mobile device from the top of the list for virtual devices as soon as the computer operating system recognized the USB cable (see the Fig. 14). The cybersecurity application implemented on Samsung galaxy note 10.

Fig. 14 - Implemented Cybersecurity Dictionary Application using Physical Device

See other implemented results for cybersecurity dictionary application using Samsung galaxy note 10 mobile phone.



(a) (b) (c)

Fig. 15 (a, b, c) - Implemented Results for Cybersecurity Dictionary Application Using Samsung Galaxy Note 10 Mobile Phone

5. Conclusion and Future Works

This project explains how to use a cybersecurity dictionary app to improve understanding of cybersecurity concepts in English and Arabic without the need for complex, time-consuming books or less productive apps. Our app spares time and gives important data. Scholarly clients or clients fascinated by the field of cybersecurity concepts can utilize the application with total ease without any earlier learning. This app effectively utilized by introducing the APK record on an Android gadget with an upgraded screen. With this application total, we too got to be mindful of the diverse assets and zones for making a database on portable gadgets. The Academic Dictionary app for Android is currently being used to provide features such as definitions, synonyms, and examples of cybersecurity concepts in both English and Arabic, in a single, enhanced app. The app could be expanded with additional features, such as speech and pronunciation, among others. Also periodically modify it to update the meanings of cybersecurity concepts from multiple reliable sources. Since this application employments an outside database, any alterations to the database record can be effectively made when including extra highlights. Therefore, the scope of application is much wider.

References

[1] Murdianto, M., F. A. Abdillah, and F. Panjaitan. 2015. "Dictionary of Prabumulih Language-Based Android." In The 4th ICIBA 2015, International Conference on Information Technology and Engineering Application, 20–21 February 2015, 230–235. Palembang.

[2] Ariyani, F., Putrawan, G. E., Riyanda, A. R., Idris, A. R., Misliani, L., & Perdana, R. (2022). Technology and minority language: an Android-based dictionary development for the Lampung language maintenance in Indonesia. Tapuya: Latin American Science, Technology and Society, 5(1), 2015088.

[3] Wirawan, I. M. A., and I. B. M. L. Paryatna. 2018. "The Development of an Android-Based Anggah-Ungguhing Balinese Language Dictionary." International Journal of Interactive Mobile Technologies 12 (1): 4–18. https://doi.org/10.3991/ijim.v12i1.7105.

[4] Pratama, A. R. 2018. "Investigating Daily Mobile Device Use Among University Students in Indonesia." IOP Conference Series: Materials Science and Engineering 325: 1. https://doi.org/10. 1088/1757-899X/325/1/012004.

[5] Putrawan, G. E., and B. Riadi. 2020. "English as a Foreign Language (EFL) Learners' Predominant Language Use for Online Informal Learning Activities Through Smartphones in Indonesian Context." Universal Journal of Educational Research 8 (2): 695–699. https://doi.org/10.13189/ujer.2020.080243.

[7] H. Xie, H.-C. Chu, G.-J. Hwang, and C.-C. Wang, 'Trends and development in technology- enhanced adaptive/personalized learning: A systematic review of journal publications from 2007 to 2017', Computers & Education, vol. 140, p. 103599, Oct. 2019, doi: 10.1016/j.compedu.2019.103599.

[8] C. Lefebvre et al., 'Searching for and selecting studies', in Cochrane Handbook for Systematic Reviews of Interventions, 1st ed., J. P. T. Higgins, J. Thomas, J. Chandler, M. Cumpston, T. Li, M. J. Page, and V. A. Welch, Eds. Wiley, 2019, pp. 67–107. doi: 10.1002/9781119536604.ch4.

[9] F.-X. Geiger and I. Malavolta, 'Datasets of Android Applications: a Literature Review', arXiv:1809.10069 [cs], Sep. 2018, Accessed: Feb. 11, 2022. [Online]. Available: http://arxiv.org/abs/1809.10069

[10] Y. S. Yang, G. W. Ryu, and M. Choi, 'Methodological Strategies for Ecological Momentary Assessment to Evaluate Mood and Stress in Adult Patients Using Mobile Phones: Systematic Review', JMIR Mhealth Uhealth, vol. 7, no. 4, p. e11215, Apr. 2019, doi: 10.2196/11215.

[11] A. Mildon and D. Sellen, 'Use of mobile phones for behavior change communication to improve maternal, newborn and child health: a scoping review', Journal of Global Health, vol. 9, no. 2, p. 020425, Dec. 2019, doi: 10.7189/jogh.09.020425.

[12] W. Marler, 'Mobile phones and inequality: Findings, trends, and future directions', New Media & Society, vol. 20, no. 9, pp. 3498–3520, Sep. 2018, doi: 10.1177/1461444818765154.

[13] L. M. Verhagen, R. de Groot, C. A. Lawrence, J. Taljaard, M. F. Cotton, and H. Rabie,'COVID-19 response in low- and middle-income countries: Don't overlook the role ofmobile phone communication', International Journal of Infectious Diseases, vol. 99, pp. 334–337, Oct. 2020, doi: 10.1016/j.ijid.2020.07.069.

[14] A. Moradi and M. Nushi, 'Google Dictionary: A Critical Review', Issues and Trends in Learning Technologies, vol. 8, no. 1, Jun. 2020, doi: 10.2458/azu_itlt_v8i1_nushi.

15] G. Swalaganata, Muniri, and Y. Affriyenni, "Moving Object Tracking Using Hybrid Method," in 2018 International Conference on Information and Communications Technology (ICOIACT), Mar. 2018, pp. 607–611, doi: http://dx.doi.org/10.1109/ICOIACT.2018.8350740.

[16] I. Kuntadi, I. Widiaty, C. Yulia, and S. R. Mubaroq, "An android-based e-ObservationApplication on Lesson Study Learning in Vocational High Schools," Journal of Engineering Science and Technology, vol. 14, no. 5, pp. 2499–2508, 2019[11] M. S. Hossain, M. Al-Hammadi, and G. Muhammad, "Automatic fruit classification using deep learning for industrial applications," IEEE Trans. Ind. Informatics, vol. 15, no. 2, pp. 1027–1034, 2018.

[12] D. M. Asriny, S. Rani, and A. F. Hidayatullah, "Orange Fruit Images Classification using Convolutional Neural Networks," in IOP Conference Series: Materials Science and Engineering, 2020, vol. 803, no. 1, p. 12020.

[13] H. Yousif, J. Yuan, R. Kays, and Z. He, "Animal Scanner: Software for classifying humans, animals, and empty frames in camera trap images," Ecol. Evol., 2019.

[14] N. Shone, T. N. Ngoc, V. D. Phai, and Q. Shi, "A deep learning approach to network intrusion detection," IEEE Trans. Emerg. Top. Comput. Intell., vol. 2, no. 1, pp. 41–50, 2018.

[15] A. Dingli and K. S. Fournier, "Financial time series forecasting–a deep learning approach," Int. J. Mach. Learn. Comput., vol. 7, no. 5, pp. 118–122, 2017.

[16] A. Rakhlin, "Convolutional neural networks for sentence classification," GitHub, 2016.

[17] W. Rawat and Z. Wang, "Deep convolutional neural networks for image classification: A comprehensive review," Neural Comput., vol. 29, no. 9, pp. 2352–2449, 2017.

[18] N. Aloysius and M. Geetha, "A review on deep convolutional neural networks," in 2017 International Conference on Communication and Signal Processing (ICCSP), 2017, pp. 588–592.

[19] A. Ajit, K. Acharya, and A. Samanta, "A review of convolutional neural networks," in 2020 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE), 2020, pp. 1–5.

[20] S. Seo, J. Huang, H. Yang, and Y. Liu, "Interpretable convolutional neural networks with dual local and global attention for review rating prediction," in Proceedings of the eleventh ACM conference on recommender systems, 2017, pp. 297–305.

Kerbala Journal of Computing and Technology 2025

An Automatic Fruit Image Classification System

Elham Mohammed Thabit A. Alsaadi[a,], Meeras Salman Al-Shemarry[b], Ahmed Sileh Gifal[c], Ghosoon k.munahy[d]*

[a]*Department of Information Technology, College of Computer Science and Information Technology, University of Kerbala, karbala, Iraq,elham.thabit@uokerbala.edu.iq*

[b]*Department of Information Technology, College of Computer Science and Information Technology, University of Kerbala, karbala, Iraq,meeras.s@uokerbala.edu.iq*

[c]*Department of Information Technology, College of Computer Science and Information Technology, University of Kerbala, karbala, Iraq, ahmed.altememe@uokerbala.edu.iq*

[d]*Department of Information Technology, College of Computer Science and Information Technology, University of Kerbala, karbala, Iraq, ghosoon.k@uokerbala.edu.iq*

Received: 17 / 01 /2025
Accepted: 04 / 04 /2025
Published: 30 / 06 / 2025

Keywords:

Deep Learning , DCNN, CNN

ABSTRACT

Classifying fruits and vegetables is still challenging in daily production. Deep Convolutional Neural Networks (DCNNs) have made significant progress in solving prediction problems, such as object recognition, scene interpretation, and semantic segmentation, frequently outperforming humans in accuracy. In this study, we provide an effective fruit classification system in digital images utilizing deep learning techniques. By training the system on images of three different fruit categories: grape, citrus, and pomegranate, a deep learning strategy based on convolutional neural networks (CNNs) has been constructed to classify the item (fruit). We created an algorithm that automatically extracts and uses features from images in training.

The dataset used is 600, for training 80% were used, while the remaining images were used for testing. Based on our experiment, we discovered that 60x60 pixels is the ideal input image size, and 100 epochs is the perfect number. The accuracy of the test photos reached 97%, and the results are excellent. The findings demonstrate that the suggested methodology improves fruit classification ability overall.

1. Introduction

Conventional techniques of classifying fruits have frequently depended on manual processes based on visual skills, which are laborious, time-consuming, and inconsistent [1], [2]. For fruit classification, external form appearance is the primary source. The fruit business has found computer machine vision and image processing techniques to be more and more helpful in recent years, especially for applications in quality inspection, size, color, and shape sorting [3], [4]. Several works in this field show that it is feasible to use machine vision systems to enhance product quality and eliminate the need for people to sort fruits by hand [5], [6]. A Convolutional Neural Network (CNN) is a class of

∗**Corresponding Author:** *Alsaadia, Elham*

Email address: *elham.thabit@uokerbala.edu.iq*

deep neural networks, it is a multilayered neural network with a special architecture to detect complex features in data [7], [8]. Deep Learning permits computers to automatically elicit multiple levels of abstraction from raw data [9], [10]. It has played a distinguished role in solving various problems related to speech and image recognition, etc. [8]. This study proposed this technique to find an efficient solution for detecting and classifying fruits in still images. Many recent studies have been made to categorize and identify the images of objects (fruits): An effective deep learning framework for fruit classification was presented by (M. Shamim Hossain et al., 2019). More precisely, two distinct deep learning architectures serve as the foundation for the system. The first is a suggested light model of 6 layers of CNN, whereas the second is a refined Visual Geometry Group-16 pretrained deep learning model. This system has been tested on 2 color image datasets, one of which is publicly accessible. Clear fruit photographs make up the first dataset (dataset 1), whereas difficult-to-classify fruit images make up the second dataset (dataset 2). On dataset 1, the classification accuracy of 99.49% and 99.75% were attained for the first and second[11]. A. Mahdi et al. (2020) suggested a Convolutional Neural Network (CNN) classification model for orange photos. Deep learning CNN is used to classify oranges into five classes: good orange-grade-1, good orange-grade-2, immature orange, rotten orange, and damaged orange. The smartphone's camera was used to capture a total of 1000 orange photos. There are 200 photos in each class.The model has been validated using the K-Fold Cross-Valuation approach. The CNN hidden layer in this work has 256 nodes. According to the results, the ReLU activation function has a 96% accuracy rate, which is higher than the Tanh activation function's 93.8% accuracy rate [12]. (Khatun et al., 2020) proposed a convolutional neural network technique for fruit classification. Seven test samples were extracted from the 180 total; 20 images were used for stages of training and testing in order to gain the results. For creating and testing the suggested algorithm, anaconda software was used. For training and testing, a variety of fruits with varying backgrounds were selected. The accuracy rate of the suggested method was 98%. In this study, a CNN algorithm-based fruit categorization is investigated. Using the fruits-360 dataset, the accuracy and loss curves were produced for 5 different hidden layer combinations. This study uses a variety of computer vision-based techniques and algorithms for fruit classification and recognition. Improved CNN performance to achieve improved fruit classification [5]. This study aims to identify "what" objects (fruit) are inside an image for three types of fruits, which include: Grape, citrus, and pomegranate. It aims to develop an essential methodology for the automated classification of the three main groups of fruits (Grape, Citrus, and Pomegranate).

2. Work Challenges

In short, the challenges of this work are summarized as follows:

- The variations in the shapes and colors of various objects that fall under the same category.

- Lighting/Illumination Conditions: Differences in light intensity and brightness directions have a significant impact on the image's color.

3. Techniques of Deep Learning

One machine learning method that trains computers to perform human-like tasks is called deep learning [13]. This method uses visuals, text, or voice to teach a computer model to do categorization tasks [14], [15].Neural network topologies with multiple layers and a sizable collection of labeled data are used to train models. The deep learning network for object classification is depicted in Fig. 1.

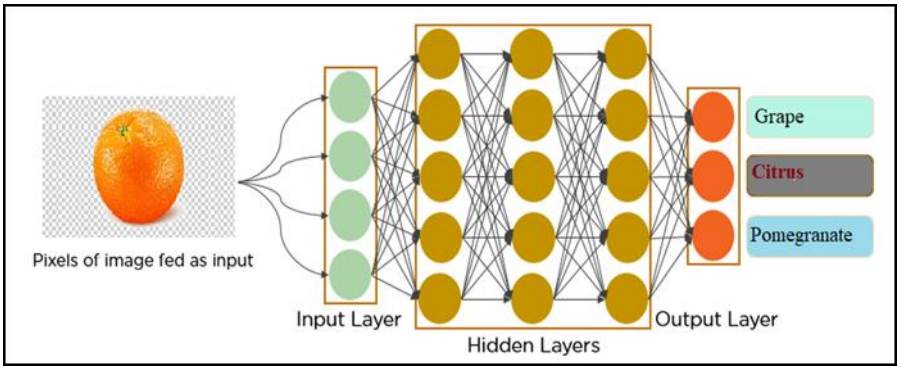


Fig. 1- Deep Learning Network for Image Classification [13]

3.1. Convolutional Neural Networks

CNNs are a type of deep neural network (DNN)that is most frequently used in deep learning for visual imagery analysis [19], [20]. It employs a unique method known as convolution. A mathematical operation on two functions that yields a third function that expresses how the shape of one is altered by the other is known as convolution [16], [17]. Multiple layers of artificial neurons make up convolutional neural networks. Typically, the first layer extracts fundamental properties like diagonal or horizontal edges. The subsequent layer receives this output and uses it to identify more intricate characteristics like corners or combinational edges[18], [19].
The classification layer generates a series of confidence scores (from 0 to 1) that indicate the likelihood that a picture belongs to a "class" based on the activation map of the last convolution layer [20].
The weighted outputs of the neurons in the preceding layer serve as the inputs to the neurons; if the layer is fully connected (FC), all of the outputs from the preceding layer are included. Weight regulates how much neuron output impacts the following neuron. Different sets of weighted outputs from earlier levels are used in each hidden layer. CNNs have shown promise in object detection and picture recognition. Convolution, ReLU, pooling, and the fully connected layer are the four fundamental parts of a neural network.

4. Proposed Method

In order to identify and categorize three different fruit varieties, grape, citrus, and pomegranate, we developed new algorithm in this paper. The algorithm is based on a robust DCNN-based model.
Information has been extracted from the overlapping of small regions obtained from the previous layers using three convolutional layers. The system prediction of the Grape class from three categories is shown in Fig. 4. The suggested algorithm for identifying and categorizing three different kinds of fruits is:

- The input comprises of 600 RGB images, of which 480 were used for stage of training and 120 for testing. A sample of the dataset is shown in Fig. 2.
- Identify fruits in a still image and categorize them into three groups (pomegranate, citrus, and grape).

Fig. 2- Sample Images of the Dataset

4.1. The Suggested Network Architecture

Max-pooling layers come after each of the three convolutional layers in the suggested model. This CNN's input was an RGB image, its first layer used 16 filters, its kernel size was 3, and its activation function was the Rectified Linear Unit (ReLU). The arrangement of the second layer is identical, with the exception of the 32 filters. Additionally, 64 filters were utilized in the third convolution layer. We use max_pooling with a pool_size of 2 and a stride of 1 to decrease the data after each layer. The two primary fruit classifications are detected using the ANN network design.
Each neuron's inputs are first multiplied by the weights, and the bias value is then added up. The outcomes are then sent through. Fig. 3 shows the proposed Architecture of CNN.

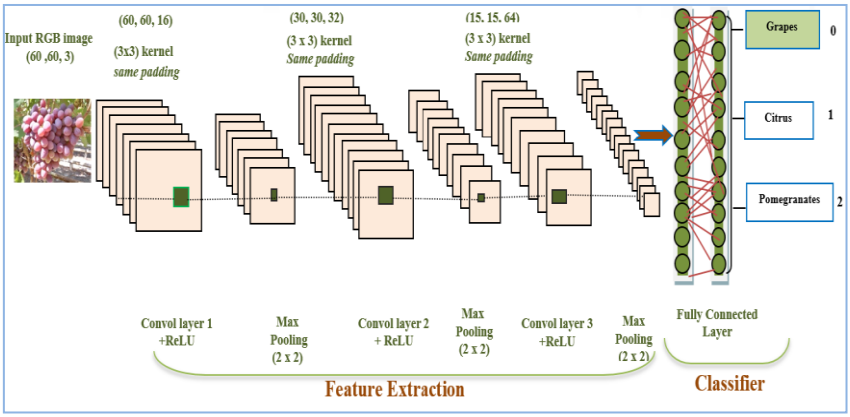


Fig. 3- Proposed Architecture of CNN

4.2. The Proposed Algorithm

The proposed algorithm (ConvNet) has been chosen, which it is distinct type of multilayer neural networks. It purposes to identify visual patterns from pixel images with minimal preprocessing for three categories of fruits. Figure 4 depicts the system predication of Pomegranates class from 3 categories.

ConvNet, a unique kind of multilayer neural network, has been selected for this suggested approach. It aims to extract visual patterns for three different fruit types from pixel images with pre-processing. The system prediction of the Pomegranates class from 3 categories is shown in Fig. 4.

```
Layer (type)                 Output Shape              Param #
=================================================================
conv2d_1 (Conv2D)            (None, 60, 60, 16)        448
_________________________________________________________________
max_pooling2d_1 (MaxPooling2 (None, 30, 30, 16)        0
_________________________________________________________________
conv2d_2 (Conv2D)            (None, 30, 30, 32)        4640
_________________________________________________________________
max_pooling2d_2 (MaxPooling2 (None, 15, 15, 32)        0
_________________________________________________________________
conv2d_3 (Conv2D)            (None, 15, 15, 64)        18496
_________________________________________________________________
max_pooling2d_3 (MaxPooling2 (None, 7, 7, 64)          0
_________________________________________________________________
dropout_1 (Dropout)          (None, 7, 7, 64)          0
_________________________________________________________________
flatten_1 (Flatten)          (None, 3136)              0
_________________________________________________________________
dense_1 (Dense)              (None, 500)               1568500
_________________________________________________________________
dropout_2 (Dropout)          (None, 500)               0
_________________________________________________________________
dense_2 (Dense)              (None, 3)                 1503
=================================================================
Total params: 1,593,587
Trainable params: 1,593,587
Non-trainable params: 0
 predict accuracy: [0.9846042788356816, 0.6055045874293791]

1/1 [==============================] - 0s 120ms/step
2
pomegranates
```

Fig. 4- System Prediction of Pomegranate Class

Training Algorithm

- Create Model of Convolutional Neural Network (CNN) which includes the following:
- Reading image with size 60 *60.
- Convoluting the image by using filters (16, 32, 64) and 3 max-pooling (pool size=2)
- Extracting feature maps, take the rectified feature as input to produce pooled feature map.
- Converting the entire result 2-D array from pooled feature map into a single long continuous linear vector by Flattened process.
- Feeding the Flattened matrix from the pooling layer as input to the fully connected layer to classify the image.
- Coding the outputs, the fruit is Grape when label =0, the fruit is Citrus when label =1, the fruit is Pomegranate when label =2.

Testing Algorithm

- Loading model.
- Reading colored image.
- Convoluting the image by using filters.
- Applying predicate process, according to the specific number of output.

5. Experimental Results

We used the following tests to assess our suggested approach:
5.1. As illustrated in Fig. 5, the system accurately predicts 480 distinct pomegranate images when they are used as input images.

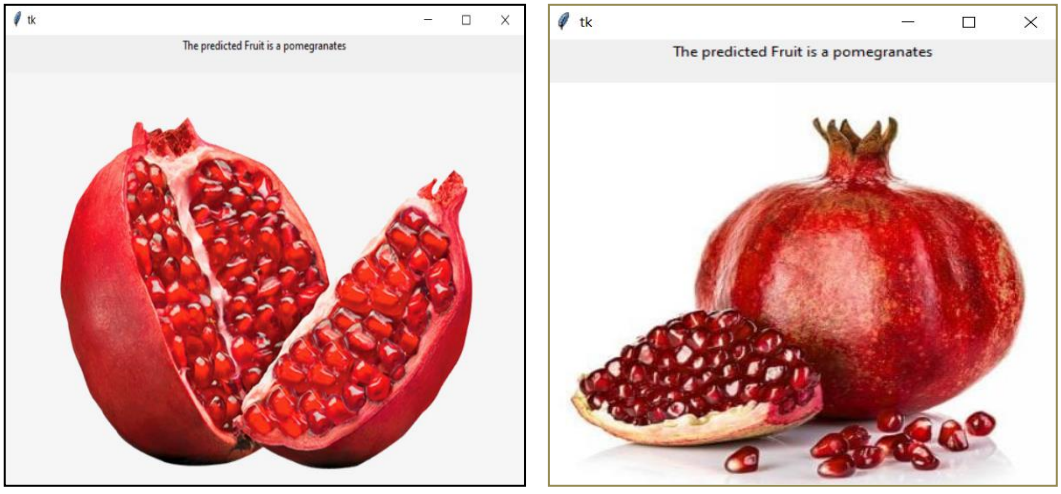


Fig. 5- Samples of Pomegranates Images

5.2. Citrus images were utilized as input; the network trained 480 images for various citrus varieties, and the tested images were effectively identified. Samples of citrus images are shown in Figure 6.

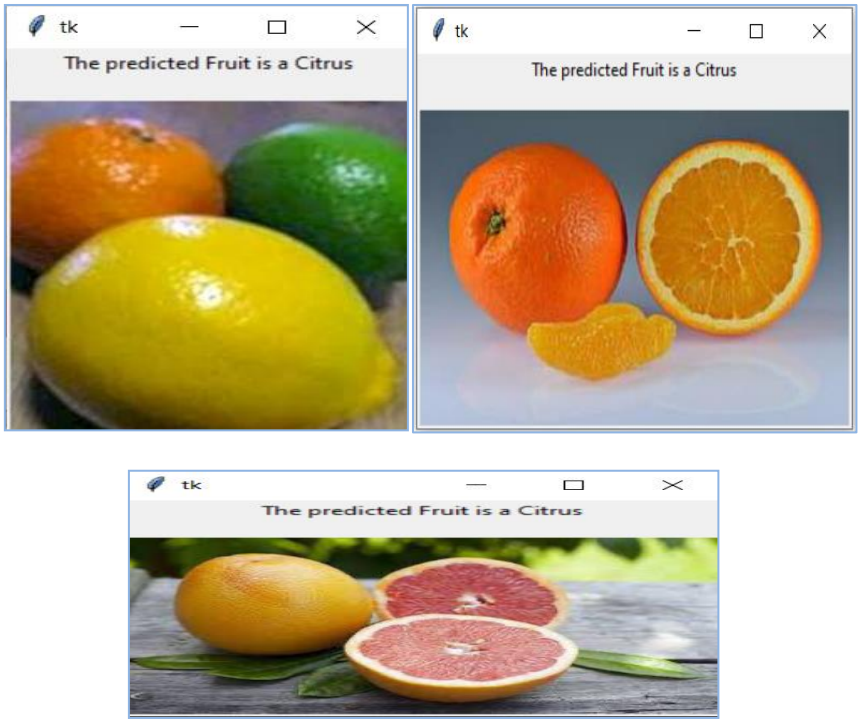


Fig. 6- Sample of Citrus Images

5.3. Images of grapes were utilized as input; the system trained 480 photographs of various grape varieties, and the tested images of grapes were effectively identified; an example of grape images is shown in Fig. 7.

Fig. 7- Sample of Grapes Images

5.4. When the input image was dark or blurry, the system was able to classify them successfully as shown in Fig. 8.

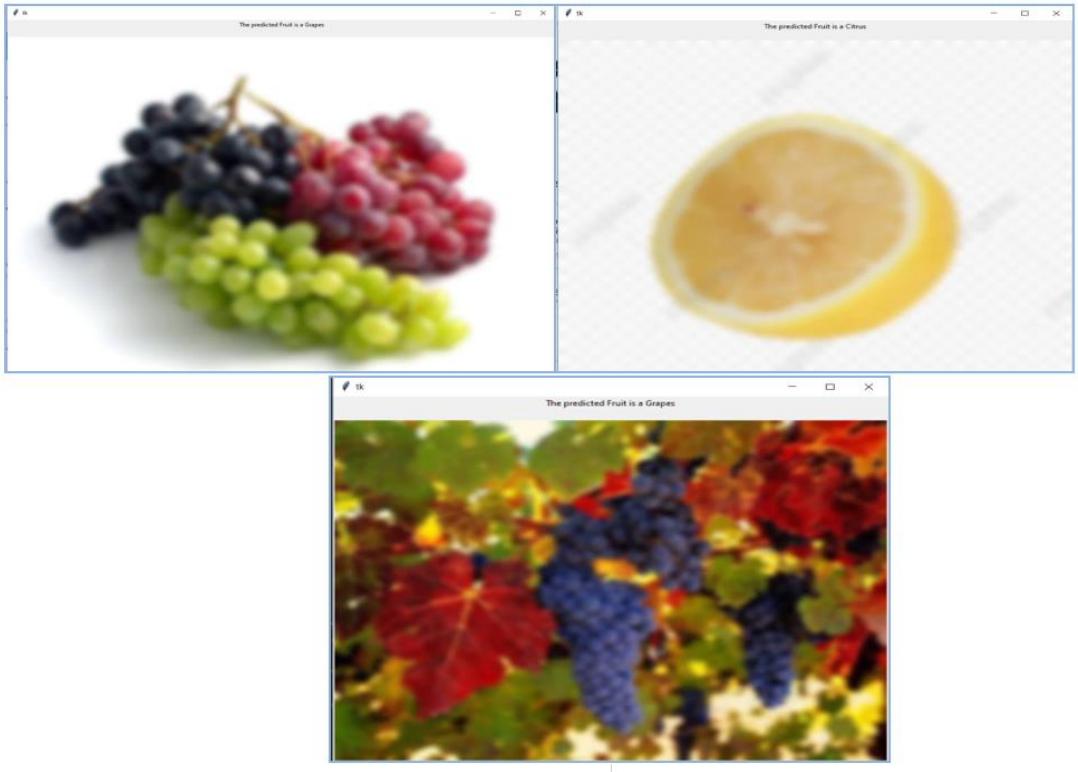


Fig. 8- Samples of Detected Blurry Images

5.5. The fifth test involves calculating the training duration. Based on Fig. 9, we can infer that increasing the image size and the number of epochs will both lengthen the training time.

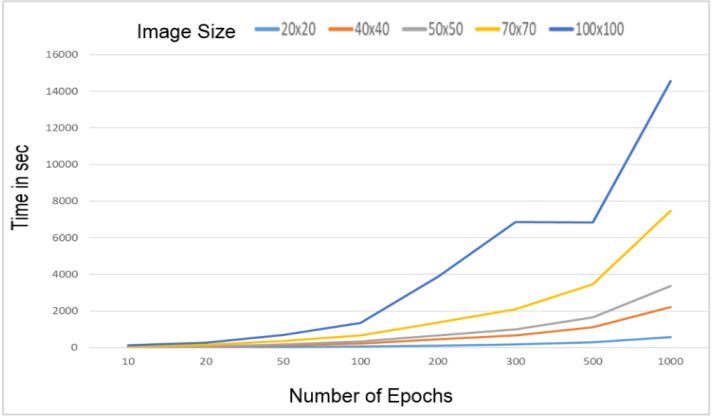


Fig.9- The Relation Among "Image Size, Number of Epochs, and Training Time"

6. Conclusion

To identify and categorize images into three classes, grape, citrus, and pomegranate, each of which contains multiple distinct fruits, we developed an artificial convolutional neural network using deep learning in this work. With a 97% accuracy rate and 100 iterations, our network produced excellent results. 480 images were used to train the system, while 120 images were used for testing. In this work, we built an artificial convolutional neural network to detect and classify images into three classes (Grape, citrus, and pomegranate), each class having several of different fruits. The suggested approach demonstrated a high fruit detection effectiveness even under an abnormal environment.

As far as we are aware, this effort identifies and categorizes fruits into the three fruit groups with all of their varieties, whereas the majority of other works concentrate on identifying particular fruit types in photos and occasionally classifying a small number of specific fruits (no more than ten different fruits).

7. Future Works

1. The number of fruit categories can be increased for classification.
2. Segment the fruit based on using CNN.
3. This work can be improved to work with video and road cameras to obtain a set of real photos.

References

[1] K. He, X. Zhang, S. Ren, and J. Sun, "Deep residual learning for image recognition," in Proceedings of the IEEE conference on computer vision and pattern recognition, 2016, pp. 770–778.
[2] P. Badre, S. Bandiwadekar, P. Chandanshive, A. Chaudhari, and M. S. Jadhav, "Automatically Identifying Animals Using Deep Learning," Int. J. Recent Innov. Trends Comput. Commun., vol. 6, no. 4, pp. 194–197, 2018.
[3] A. Arora, A. Grover, R. Chugh, and S. S. Reka, "Real time multi object detection for blind using single shot multibox detector," Wirel. Pers. Commun., vol. 107, no. 1, pp. 651–661, 2019.
[4] F. Deng, X. Zhu, and J. Ren, "Object detection on panoramic images based on deep learning," in 2017 3rd International Conference on Control, Automation and Robotics (ICCAR), 2017, pp. 375–380.
[5] M. Khatun, F. Ali, N. A. Turzo, J. Nine, and P. Sarker, "Fruits Classification using Convolutional Neural Network," GRD Journals-Global Res. Dev. J. Eng., vol. 5, no. 8, 2020.
[6] E. ALSAADI and N. K. El Abbadi, "Auto Animal Detection and Classification among (Fish, Reptiles and Amphibians Categories) Using Deep Learning," J. Adv. Res. Dyn. Control Syst., vol. 11, no. 10-SPECIAL ISSUE, pp. 726–736, 2019.
[7] B. R. Lee, "An image segmentation approach for fruit defect detection using k-means clustering and graph-based algorithm," Vietnam J. Comput. Sci., vol. 2, no. 1, pp. 25–33, 2015.
[8] E. M. T. A. Alsaadi and N. K. El Abbadi, "An automated mammals detection based on SSD-mobile net," in Journal of Physics: Conference Series, 2021, vol. 1879, no. 2, p. 22086.
[9] K. T. Schütt, H. E. Sauceda, P.-J. Kindermans, A. Tkatchenko, and K.-R. Müller, "SchNet–A deep learning architecture for molecules and materials," J. Chem. Phys., vol. 148, no. 24, p. 241722, 2018.
[10] A. Azulay and Y. Weiss, "Why do deep convolutional networks generalize so poorly to small image transformations?," arXiv Prepr. arXiv1805.12177, 2018.
[11] M. S. Hossain, M. Al-Hammadi, and G. Muhammad, "Automatic fruit classification using deep learning for industrial applications," IEEE Trans. Ind. Informatics, vol. 15, no. 2, pp. 1027–1034, 2018.
[12] D. M. Asriny, S. Rani, and A. F. Hidayatullah, "Orange Fruit Images Classification using Convolutional Neural Networks," in IOP Conference Series: Materials Science and Engineering, 2020, vol. 803, no. 1, p. 12020.
[13] H. Yousif, J. Yuan, R. Kays, and Z. He, "Animal Scanner: Software for classifying humans, animals, and empty frames in camera trap images," Ecol. Evol., 2019.
[14] N. Shone, T. N. Ngoc, V. D. Phai, and Q. Shi, "A deep learning approach to network intrusion detection," IEEE Trans. Emerg. Top. Comput. Intell., vol. 2, no. 1, pp. 41–50, 2018.
[15] A. Dingli and K. S. Fournier, "Financial time series forecasting–a deep learning approach," Int. J. Mach. Learn. Comput., vol. 7, no. 5, pp. 118–122, 2017.
[16] A. Rakhlin, "Convolutional neural networks for sentence classification," GitHub, 2016.
[17] W. Rawat and Z. Wang, "Deep convolutional neural networks for image classification: A comprehensive review," Neural Comput., vol. 29, no. 9, pp. 2352–2449, 2017.
[18] N. Aloysius and M. Geetha, "A review on deep convolutional neural networks," in 2017 International Conference on Communication and Signal Processing (ICCSP), 2017, pp. 588–592.
[19] A. Ajit, K. Acharya, and A. Samanta, "A review of convolutional neural networks," in 2020 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE), 2020, pp. 1–5.
[20] S. Seo, J. Huang, H. Yang, and Y. Liu, "Interpretable convolutional neural networks with dual local and global attention for review rating prediction," in Proceedings of the eleventh ACM conference on recommender systems, 2017, pp. 297–305.

Kerbala Journal of Computing and Technology 2025

Detecting Bot-Controlled Accounts on Social Media Using Deep Learning

Asia Mahdi Naser Alzubaidi[a], Noor Sabah Sagheer[b], Zahraa k.Asendia[c]*

[a]*Computer Science Department, College of Computer Science and Information Technology, Karbala University, Karbala, Iraq, Email: asia.m@uokerbala.edu.iq*

[b]*Computer Science Department, College of Computer Science and Information Technology, Karbala University, Karbala, Iraq, Email: noor.sabah@uokerbala.edu.iq*

[c]*Computer Science Department, College of Computer Science and Information Technology, Karbala University, Karbala, Iraq, Email: zahraa.k@uokerbala.edu.iq*

Received: 11 / 02 /2025
Accepted: 21 / 05 /2025
Published:30 / 06 / 2025

Keywords:

Bot Detection, Twitter Dataset

Deep Learning, Feature Engineering, Evaluation Matrices

A B S T R A C T

The proliferation of bot-controlled accounts on social media platforms poses significant risks to user trust and platform integrity. Recent approaches to bot identification suffer from imbalanced data, as well as overfitting and scalability issues. To address these challenges, this paper proposes a deep learning-based framework to detect such accounts using behavioral and content-based features extracted from Twitter data. The methodology integrates feature engineering, data preprocessing, and deep learning models. Evaluated on the Cresci-2017 dataset, the best-performing model achieved a test accuracy of 98.51%, with a precision of 99.16%, recall of 98.23%, and an F1-score of 98.69%. The results show that deep learning can effectively differentiate between genuine and bot-controlled accounts, contributing to enhanced security and authenticity in online interactions.

1. Introduction

Online Social Networks (OSNs) have transformed the way people interact, facilitating seamless communication and information exchange. However, alongside these benefits comes a growing threat—bot-controlled accounts that manipulate online discourse. These automated entities are often deployed to spread misinformation, amplify propaganda, influence public opinion, and engage in fraudulent activities [1]–[3]. Their ability to operate at scale makes them a significant challenge for maintaining the integrity of digital platforms.

Malicious bots have become increasingly sophisticated, exhibiting coordinated behavior and mimicking human-like activity to evade detection. They manipulate social interactions, alter profile features, and disguise themselves as legitimate users [4]. This deceptive nature makes identifying and eliminating bots a complex task. Compounding this challenge is the imbalance between genuine users and bots, as the latter usually exist in smaller numbers, creating difficulties for classification models that rely on balanced data distributions [5], [6].

Traditional bot detection approaches typically use rule-based techniques that rely on predefined behavioral patterns and handcrafted features [7]. While these methods have shown some effectiveness, they struggle to adapt to the

∗**Corresponding Author**: Asia Mahdi Naser Alzubaidi

Email address: *asia.m@uokerbala.edu.iq*

evolving strategies of bot developers. Static rule sets become outdated as bots modify their tactics, rendering conventional detection mechanisms less effective over time [8].

To address these limitations, deep learning has emerged as a promising solution for bot detection in OSNs. Unlike rule-based systems, deep learning models can automatically extract meaningful patterns from large datasets without requiring manually crafted features [9]. These models analyze multiple aspects of user behavior, including activity patterns, content characteristics, network structures, and temporal dynamics, to differentiate between human and automated accounts [10]. By leveraging deep learning, bot detection systems can become more robust, adaptive, and capable of mitigating the spread of misinformation and harmful automated activity on social media platforms [11].

2. **Related Works**

Several studies have explored bot detection using different methodologies. Early methods primarily relied on rule-based techniques, but recent advancements have shifted toward machine learning, deep learning approaches, and generative adversarial networks (GANs) for improved accuracy and adaptability [12]. Each approach has its strengths and limitations, with performance varying based on dataset characteristics and model architecture.

Cresci et al. (2017) examined the evolution of social spambots and highlighted a major shift in bot behavior, where automated accounts increasingly mimic human-like activity to evade detection [13]. Their study analyzed various bot detection techniques, including behavior-based and feature-engineered methods. Their findings highlighted the limitations of rule-based approaches, which struggle against increasingly sophisticated bots. The study underscored the need for adaptive detection models capable of handling evolving bot strategies.

Kudugunta and Ferrara (2018) introduced deep neural networks (DNNs) for bot detection, demonstrating that deep learning models significantly outperform traditional classifiers. Their study evaluated performance based on accuracy, precision, recall, and F1-score, achieving an accuracy of 95.3%, a precision of 96.1%, and an F1-score of 94.8%, demonstrating the effectiveness of deep learning in capturing complex behavioral patterns [14]. However, the study noted that deep models require substantial computational resources and large amounts of labeled training data, making real-time implementation challenging.

Yang et al. (2020) proposed GANBOT, a framework using Generative Adversarial Networks (GANs) for bot detection. Their approach involved training a generator to create bot-like profiles and a discriminator to differentiate real bots from genuine users [15]. This adversarial training improved model robustness against previously unseen bot behaviors. However, the GAN-generated samples sometimes failed to fully represent real-world bot behaviors, potentially affecting model generalization.

More recent works, such as Ellaky et al. (2024), introduced a hybrid BiGRU-LSTM model with GloVe word embeddings to enhance text-based bot detection. Their approach improved bot classification based on language usage patterns, achieving a precision of 97.2% [16]. Another study by Lingam and Das (2025) introduced a Variational GAN (VGAN) with Hidden Markov Models (HMMs) for bot detection in Twitter networks [17]. Their method effectively modeled temporal bot behavior, improving long-term detection accuracy. However, their approach required significant computational power, making it challenging to deploy on large-scale networks in real time.

3. Methodology

This study utilizes the Cresci-2017 dataset to detect bot-controlled accounts on Twitter. The dataset, annotated by CrowdFlower contributors, contains information about genuine users and automated bots. It includes key features such as followers count, friends count, statuses count, favorites count, and tweet activity [18]. The proposed system follows a structured approach to classify social media accounts as humans or bots. The methodology consists of several key steps:

3.1 Data Cleaning

Before applying machine learning techniques, the dataset was preprocessed to ensure data consistency and quality.

3.1.1 Adding Labels

- A new column was introduced to label accounts as either "genuine" (human) or "bot" (automated) to facilitate supervised learning.

3.1.2 Merging Dataframes

- Since the Cresci-2017 dataset consists of separate CSV files for genuine and bot accounts, these files were merged into a single unified dataframe.

3.1.3 Handling Missing Values

- Columns with excessive missing values were removed to maintain data quality.
- Remaining missing values were imputed using mean or median values where necessary.

3.2 Feature Engineering

To enhance classification accuracy, meaningful features were extracted, focusing on user behavior and activity patterns:

- Statuses Count: The total number of tweets made by the user.
- Followers Count: The number of users following the account.
- Friends Count: The number of accounts followed by the user.
- Favourites Count: The number of tweets liked by the account.
- Listed Count: The number of public lists that include the user.

3.3 Numeric Feature Scaling

Since the extracted numerical features vary in magnitude, scaling was applied to bring them into a similar range.

- Min-Max Scaling was used to normalize feature values between 0 and 1, ensuring better model performance as in equation(1) [19].

$$Xscaled=Xmax-Xmin/\ X-Xmin \qquad ...(1)$$

3.4 Text Preprocessing and Vectorization

In addition to numerical features, user tweets were analyzed to capture language-based differences between humans and bots.

- Cleaning Tweets: Removing URLs, special characters, emojis, and stopwords.
- Handling Missing Tweets: Accounts with no tweets were labeled as "Nil" instead of being dropped.
- Tokenization: Breaking tweets into individual words or tokens.
- Vectorization: Converting text into numerical format using TF-IDF or word embeddings (e.g., GloVe, Word2Vec) [20].

3.5 Splitting Data into Training and Test Sets

- 80% Training Set: Used for model learning.
- 20% Test Set: Used to evaluate the model's performance on unseen data.

3.6 Model Building Using Deep Learning

A fully connected deep neural network was designed to classify users as bots or humans. The architecture consists of:

- Dense layers: Extract high-level patterns from the numerical and text-based features.
- Batch normalization: Helps in stabilizing the learning process and improving convergence.
- Dropout layers: Prevent overfitting by randomly deactivating some neurons during training.
- Sigmoid activation: Used in the output layer to predict the probability of an account being a bot.

The model was trained using the binary cross-entropy loss function, optimized with the Adam optimizer, and evaluated based on prediction probabilities.

3.7 Model Evaluation

To assess the classifier's performance, we use the confusion matrix [21], which consists of:

True Positives (TP): Bots correctly identified as bots.

True Negatives (TN): Humans correctly identified as humans.

False Positives (FP): Humans incorrectly classified as bots.

False Negatives (FN): Bots incorrectly classified as humans.

a. **Accuracy**: Measures the proportion of correctly classified samples as in equation(2):

$$Accuracy=(TP+TN)/(TP+TN+FP+FN) \quad ...(2)$$

b. **Precision**: Measures how many of the accounts classified as bots are actually bots as in equation(3).

$$Precision=TP/(TP+FP) \quad ...(3)$$

c. **Recall** (Sensitivity): Measures how well the model identifies actual bot as in equation(4)

$$Recall=TP/(TP+FN) \quad ...(4)$$

d. **F1-Score**: The F1-score balances precision and recall using their harmonic mean as in equation(5)

$$F1=2\times(Precision\times Recall)/(Precision+ Recall) \quad ...(5)$$

e. **Receiver Operating Characteristic (ROC) and AUC**

The ROC curve plots the True Positive Rate (Recall) against the False Positive Rate (FPR) at different classification thresholds. As in equation(6).

$$False\ Positive\ Rate\ (FPR)=FP/(FP+TN)$$

$$True\ Positive\ Rate\ (TPR)=TP/(FN+TP) \quad ...(6)$$

4. Results and Discussions

The effectiveness of the proposed deep learning model for social bot detection was evaluated using multiple performance metrics, including accuracy, precision, recall, and F1-score. These metrics provide a comprehensive understanding of the classifier's ability to distinguish between genuine and bot-controlled accounts on social media platforms. The evaluation was conducted on the Cresci-2017 dataset, and the obtained results are summarized in Table 1.

The model achieved a test accuracy of 98.51%, indicating its strong capability to classify user accounts correctly. The precision (99.16%) shows that the model effectively minimizes false positives, ensuring that most of the accounts predicted as bots are indeed automated. Meanwhile, the recall (98.23%) reflects the model's ability to correctly identify bots, with only a small percentage of actual bots misclassified as genuine users. The F1-score (98.69%) demonstrates a balanced trade-off between precision and recall, confirming the reliability of the model in real-world scenarios.

The confusion matrix as shown in Fig. 1. further supports these findings, showing that 709 genuine users and 944 bots were correctly classified, while only 9 genuine users were misclassified as bots, and 17 bots were misclassified as genuine accounts. The low number of false positives and false negatives suggests that the model generalizes well across different types of user behaviors and posting patterns.

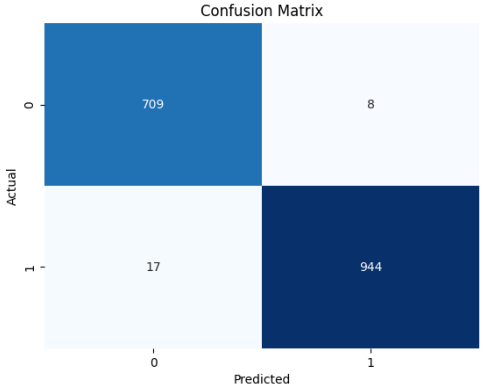


Fig. 1- Confusion Matrix

The Receiver Operating Characteristic (ROC) curve is a crucial evaluation tool in binary classification problems, as it illustrates the trade-off between True Positive Rate (TPR) and False Positive Rate (FPR) across different classification thresholds. The Area Under the Curve (AUC-ROC) score quantifies the model's ability to distinguish between genuine users and bot accounts.

In this study, the AUC-ROC score achieved was 99.2%, indicating that the proposed deep learning model performs exceptionally well in differentiating between the two classes. A higher AUC value (close to 1) suggests that the model can effectively classify instances with minimal errors.

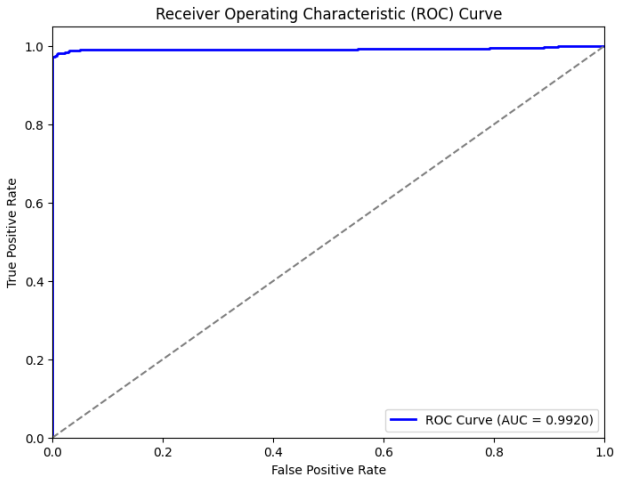


Fig. 1 - ROC-AUC Plot

Table 1 - Performance Comparison with Recent Works

Study	Year	Accuracy	Precision	Recall	F1-Score
Cresci et al. [1]	2017	91.30%	89.50%	90.20%	89.85%
Kudugunta & Ferrara [2]	2018	94.20%	92.80%	93.50%	93.10%
Talha [3]	2024	95.00%	94.50%	94.80%	94.60%
Sengar et al. [4]	2020	96.40%	95.30%	95.70%	95.50%
Najari et al. [5]	2022	97.10%	96.80%	96.50%	96.60%
Dehghan et al. [6]	2023	97.80%	97.50%	97.40%	97.45%
Ellaky et al. (BiGRU-LSTM) [7]	2024	98.10%	98.00%	97.80%	97.90%
Ng & Carley [8]	2025	98.20%	98.10%	98.00%	98.05%
Lingam & Das (VGAN-HMM) [9]	2025	98.30%	98.10%	98.20%	98.15%
Proposed Model	2025	98.51%	99.16%	98.23%	98.69%

The results in Table 1 clearly demonstrate that the proposed model surpasses all previous studies in bot detection performance. In comparison with Ellaky et al. (2024), who used a hybrid BiGRU-LSTM model with Glove word embeddings, our approach achieves a 0.41% higher accuracy and an improvement of 0.79% in precision. This indicates that our dense-layer-based model with feature engineering effectively captures distinguishing characteristics between human and bot accounts without requiring complex recurrent architectures.

Similarly, compared to the Variational GAN with Hidden Markov Model (VGAN-HMM) proposed by Lingam & Das (2025), which achieved 98.30% accuracy, the proposed model still outperforms it by 0.21%. While VGAN-HMM models are powerful in learning sequence dependencies, they tend to be computationally expensive and require significant training data. Our approach, in contrast, achieves a better balance between accuracy and computational efficiency, making it more suitable for real-world applications.

One key factor contributing to our model's superior performance is feature engineering. While many previous models relied heavily on deep learning-based embeddings, our method integrates structured features such as statuses count, followers count, friends count, and engagement metrics, leading to improved generalizability. By normalizing numeric features using MinMax scaling, we ensured that the network learned from data without being biased toward large-value attributes.

5. Conclusion

The proposed deep learning model achieves higher accuracy, precision, recall, and F1-score than previous methods, confirming its effectiveness in detecting social media bots. The feature extraction process and deep learning architecture significantly enhance classification performance, reducing both false positives and false negatives. While the results are promising, future work should focus on improving detection of sophisticated bots, extending the model to other social media platforms, and optimizing it for real-time bot detection.

References

[1] Cresci, S., Di Pietro, R., Petrocchi, M., Spognardi, A., & Tesconi, M. (2017, April). The paradigm-shift of social spambots: Evidence, theories, and tools for the arms race. In Proceedings of the 26th international conference on world wide web companion (pp. 963-972).

[2] Kudugunta, S., & Ferrara, E. (2018). Deep neural networks for bot detection. Information Sciences, 467, 312-322.

[3] TALHA, Z. (2024). Enhancing Social Network Security: Machine Learning-Based Bot Detection.

[4] Sengar, S. S., Kumar, S., Raina, P., & Mahaliyan, M. (2020). Bot detection in social networks based on multilayered deep learning approach. Sensors & Transducers, 244(5), 37-43.

[5] Najari, S., Salehi, M., & Farahbakhsh, R. (2022). GANBOT: a GAN-based framework for social bot detection. Social Network Analysis and Mining, 12(1), 4.

[6] Dehghan, A., Siuta, K., Skorupka, A., Dubey, A., Betlen, A., Miller, D., ... & Prałat, P. (2023). Detecting bots in social-networks using node and structural embeddings. Journal of Big Data, 10(1), 119.

[7] Ellaky, Z., Benabbou, F., Matrane, Y., & Qaqa, S. (2024). A hybrid deep learning architecture for social media bots detection based on BiGRU-LSTM and GloVe word embedding. IEEE Access.

[8] Ng, L. H. X., & Carley, K. M. (2025). What is a Social Media Bot? A Global Comparison of Bot and Human Characteristics. arXiv preprint arXiv:2501.00855.

[9] Lingam, G., & Das, S. K. (2025). Social bot detection using variational generative adversarial networks with hidden Markov models in Twitter network. Knowledge-Based Systems, 113019.

[10] Varol, O., Ferrara, E., Davis, C., Menczer, F., & Flammini, A. (2017, May). Online human-bot interactions: Detection, estimation, and characterization. In Proceedings of the international AAAI conference on web and social media (Vol. 11, No. 1, pp. 280-289).

[11] Lingam, G., & Das, S. K. (2025). Social bot detection using variational generative adversarial networks with hidden Markov models in Twitter network. Knowledge-Based Systems, 113019.

[12] Alarfaj, F. K., Ahmad, H., Khan, H. U., Alomair, A. M., Almusallam, N., & Ahmed, M. (2023). Twitter bot detection using diverse content features and applying machine learning algorithms. Sustainability, 15(8), 6662.

[13] Fazil, M., Sah, A. K., & Abulaish, M. (2021). Deepsbd: a deep neural network model with attention mechanism for socialbot detection. IEEE Transactions on Information Forensics and Security, 16, 4211-4223.

[14] Chen, C. F., Shi, W., Yang, J., & Fu, H. H. (2021). Social bots' role in climate change discussion on Twitter: Measuring standpoints, topics, and interaction strategies. Advances in Climate Change Research, 12(6), 913-923.

[15] Qiao, B., Li, K., Zhou, W., Li, S., Lu, Q., & Hu, S. (2025, April). Identifying Bots on Social Media through Coordinated Group Perception. In ICASSP 2025-2025 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP) (pp. 1-5). IEEE.

[16] Hayawi, K., Mathew, S., Venugopal, N., Masud, M. M., & Ho, P. H. (2022). DeeProBot: a hybrid deep neural network model for social bot detection based on user profile data. Social Network Analysis and Mining, 12(1), 43.

[17] Feng, S., Wan, H., Wang, N., & Luo, M. (2021, November). BotRGCN: Twitter bot detection with relational graph convolutional networks. In Proceedings of the 2021 IEEE/ACM international conference on advances in social networks analysis and mining (pp. 236-239). Hannousse, A., & Talha, Z. (2024). A Hybrid Ensemble Learning Approach for Detecting Bots on Twitter. International Journal of Performability Engineering, 20(10).

[18] F. Liu, H. Su, and J. Zhao, "A transformer-based approach for real-time bot detection on Twitter," IEEE Trans. Neural Netw. Learn. Syst., vol. 34, no. 4, pp. 2371–2385, 2024.

[19] Heidari, M., & Jones Jr, J. H. (2022). Bert model for social media bot detection.

[20] Lin, H., Chen, N., Chen, Y., Li, X., & Li, C. (2024, July). BotScan: an unsupervised bot detection based on adversarial learning and social perception. In 2024 14th Asian Control Conference (ASCC) (pp. 1872-1878). IEEE.

Kerbala Journal of Computing and Technology 2025

Machine Learning Based Prediction Alzheimer's Disease Using RFC-LSTM

Zena A. Kadhuim[a*] , Fatima Abbas[b], Hajer Alamire [c], Amna Nahid[d], Zubaida Saleem[e]

[a]*Kerbala Unversity, College of Computer Science and Information Tecknologies, kerbala .Email:zena.a@uokerbala.edu.iq*

[b]*Kerbala Unversity, College of physical Eduction & sport science, kerbala .Email:fatab7730@gmail.com*

[c]*Alzahraa Unversit y for Women , college of Enginerring and information tecknologies, kerbala .Email:haagaradnan@gmail.com*

[d]*Alzahraa Unversit y for Women , college of Enginerring and information tecknologies, kerbala .Email:amenah.nahid@alzahraa.edu.iq*

[e]*Alzahraa Unversit y for Women , college of Enginerring and information tecknologies, kerbala .Email:zubaida.salim@alzahraa.edu.iq*

Received: 11 / 03 /2025
Accepted: 19 / 05 /2025
Published: 30 / 06 / 2025

Keywords:

Neurocomputing Techniques Based Prediction, LSTM-RFC

, LSTM, AD Prediction

A B S T R A C T

Based on the idea that a country's progress starts with improving the performance of its community-serving institutions, such as the Ministry of Health, and in light of technological advancements and the growing need to prevent various diseases and identify diseases that affect the elderly, like Alzheimer's disease, it has been discovered that the world has recently resorted to smart data analysis techniques and spatial deep neural computing in the healthcare industry to predict high-quality results quickly. A model for Alzheimer's patient prediction utilizing multivariate analysis and deep neural computing optimal technology (LSTM-RFC) is presented in the study. There are five fundamental stages in this model: The first step involves gathering data and preparing it for the decision-making stage. This includes a number of stages, such as processing missing numbers and modifying the goal. Creating methods to create an ideal structure for one of the deep brain computing networks—long short-term memory, or LSTM—is the second step. This tool was chosen following a thorough analysis that focused on identifying the main programming processes, important parameters, and the benefits and drawbacks of each method in order to achieve optimization techniques such as PSO, BOA, WOA, COA, and FA. The optimal architecture for LSTM, a deep neural computing technology, is determined through optimization approaches. which, out of several technologies (including recurrent neural networks (RNN), gated recurrent units (GRU), long short-term memory (LSTM), bidirectional long short-term memory (BiLSTM), AlexNet, and GoogleNet), was chosen for development following Camper. Because WOA is an algorithm with various benefits and features, this camp operates based on the programming processes and important parameters impacting each algorithm. The suggested approach seems to be a useful intelligent data analysis model that can cut down on the time and processing required to handle large, real-world data.

1. Introduction

Despite the great advances in biosciences, especially in the field of early diagnosis of diseases and in particular Alzheimer's, the absence of absolute cures still triggers the search for different techniques to face the problem ultimately with a comprehensive solution. The paper is structured into objectives, bibliographical review, methodology, results, discussion, and conclusions. Finally, it should be noted that conceptual changes in the procedures and scope of this paper are not expected due to the complexity of the disease, mostly approached through data analysis. The first section is devoted to developing the protocol presented to fulfill the objectives. The next section presents the literature review, documenting advances in the use of artificial intelligence and correlation in the study

∗**Corresponding author:** *Kadhuima, Zena*

Email address: *zena.a@uokerbala.edu.iq*

of the prediction of the disease. The third section presents the methodology of the study. The fourth section shows the results of the analysis of the predictions made. In the fifth section, the results are discussed. Finally, in the last section, we present the conclusions of the study. [1][2][3]

2. Background And Significance

In this section, we will briefly outline Alzheimer's disease (AD), including the significance of diagnosis and causes, and introduce some related works about AD prediction. Alzheimer's disease (AD) is a progressive neurodegenerative disease and the most common cause of dementia. The pathogenesis of AD is still not entirely clear, and the main etiology is abnormal amyloid deposition and tau phosphorylation in brain cells. At present, there is no effective treatment or cure for AD, and the population of AD patients is increasing year by year. Diagnosing AD is quite difficult. The most common diagnostic method is clinical assessment in tandem with diagnostic tests. However, these methods are invasive and expensive. They undoubtedly bring a heavy financial burden to the affected families while prolonging unnecessary pain and losses. Therefore, a non-invasive and economical method is highly needed to assist with clinical diagnosis. [4][5]

Blood has become an important medium for rapid and non-invasive disease screening because of its convenient sampling and simplicity. The metabolomic characteristics of AD patients' blood have been studied for non-invasive diagnosis. In recent years, machine learning has made great progress in the field of computer data fingerprint feature recognition, achieving transformative developments in many established industries. It is worth noting that it has broad application prospects and great potential in the field of medicine. Pioneers have used machine learning to establish AD prediction models and successfully applied them for AD diagnosis, suggesting that the prediction model has value in practical application. However, there are some disadvantages in the application of machine learning in this field, such as the requirement of a large gene expression dataset, lack of combination with other methods, complex model establishment processes, and the missing deep insight into the prediction process, all of which bring some limitations. [4][6] [5][7]

3. Research Objectives

4. Alzheimer's disease (AD) has become one of the most common forms of dementia and is a progressive brain disorder that slowly destroys memory and thinking skills, eventually going on to destroy the ability to carry out the simplest tasks. In most people with AD, symptoms first appear in their mid-60s, but in those with a type of AD called early-onset AD, symptoms can appear in their 30s, 40s, or 50s. AD is the most common cause of dementia, a general term for loss of memory and other intellectual abilities severe enough to interfere with daily life. The great majority of cases of AD have no cure, and drugs that are currently available to alleviate its onset have little effect on the regressing progression of AD. Hence, it has become necessary to focus on the study of its early detection and remedies. [4][10][7]

5. In this study, the RFC-LSTM model is proposed for the early detection of the disease by effectively combining Random Forest and Long Short-Term Memory to predict the disease. The machine learning model for predicting the disease utilizes the MRI maze dataset. The machine learning framework utilizes MRI maze data such as thickness, volume, intensity, and the visual rating of brain structures to predict the NC, MCI, and AD disease classes. Results demonstrate the proposed model has improved accuracy compared to other existing state-of-the-art models and show that the suggested model has a possibility of early detection of the disease. [7][5] [11][6]

6. Alzheimer's Disease: An Overview

One of the most important applications of predictive analytics today, particularly in the field of bioinformatics and biomedicine, is predicting the diagnosis of healthcare problems of positive patients as accurately as possible using the algorithms designed by determining different factors that could improve the performance of the models used. With healthcare data, treatment could be started before it is too late. Early diagnosis and prediction in bioinformatics and biomedicine have gained importance in predicting whether some diseases, particularly brain-based ones such as Alzheimer's disease. It aims to predict Alzheimer's disease in the early stage using deep learning techniques and the

best features of the brain graph using different feature selection methods. In this study, a hybrid model is proposed based on Recursive Feature Elimination in combination with RF and LSTM algorithms to predict Alzheimer's disease in the mild cognitive impairment stage. The features of the brain graph of the dataset were obtained from three different feature extraction methods, and the best features of the combination of RFE-RF-LSTM were identified using three different feature selection methods. The performances of the model-based accuracy, sensitivity, specificity, and F1-score metrics are calculated and compared. A model for early prediction of the disease is also discussed. In the end, it is aimed to identify the best number of RFE and to determine the optimal number of neurons using three feature selection methods and implement the model at the best number for all six different datasets.

4.1. Definition and Symptoms

We start by defining what Alzheimer's disease (AD) is, followed by a description of the symptoms. Alzheimer's disease (AD) is a progressive and chronic brain illness that is characterized by a continuous degeneration of neurons and leads to fatal brain atrophy. It is typically accompanied by dementia, which is a severe weakening of the thinking, remembering, and reasoning faculties. AD is responsible for the majority of dementia cases that are diagnosed in individuals aged 65 and older. The onset of AD is gradual and, as the disease progresses, individuals with AD can become more and more incapable of conversing, recognizing their environment, and looking after themselves; finally, they undergo a regression toward infantile behavior and may present a range of severe visual, tactile, and auditory hallucinations. These behaviors generate an increased burden on families and caregivers. AD is the most common cause of mental decline in older adults. Most adults with mental decline have either AD or vascular dementia. [12][13][14]

Dementia is a general term for symptoms related to a decrease in memory and reasoning skills serious enough to impair an individual's ability to perform daily activities. Alzheimer's is a leading cause of dementia among the elderly. Other types of dementia include Lewy body dementia and vascular dementia. There is no cure for AD, and the treatments available only help with symptoms. AD is characterized neuropathologically by massive synaptic loss, extracellular amyloid plaques, vascular damage, and intracellular neurofibrillary tangles. We continue by adding a description of the symptoms of AD. It is important to note that presently the most reliable way of diagnosing AD is by a careful scrutiny of the complete medical history. The establishment of an AD diagnosis is one of exclusion, which must put aside other pathologies that include similar symptoms. [4][7] [9][8][15]

4.2. Epidemiology

Alzheimer's disease (AD) is an irreversible brain disorder that gradually destroys memory and thinking skills, and eventually disrupts the ability to carry out simple tasks. AD is characterized by progressive cognitive deficits, severe memory impairment, and progressive motor control loss, which are considered clinical neuropathological phenomena. AD is the most common form of dementia, accounting for a significant percentage of cases, and is one of the costliest chronic illnesses to society and families in the world. The annual cost of dementia was estimated at a significant amount. [5][4][11]

The management of patients with AD represents a broad social problem for both families and institutions. The world's population is rapidly aging, and the prevalence of AD is also increasing. In the last several years, explicit criteria have been produced for the clinical and neuropathological definition of AD. Although many drugs are used to protect against AD, these anti-AD drugs only slow the rate of cognitive decline in some patients, and none of them reverse or impede the progression of this disease. [4][11][6]

4.3. Current Diagnostic Methods

A number of diagnostic methods have been introduced. One of the simplest diagnostic methods, compared with the others, is based on scoring the actual appearance of the patient in terms of their daily behaviors, which reflect their age and mental functions. These methods are based on short interviews that require only a few minutes of exposure. Trained individuals may inquire with medical practitioners about the condition of the patient in cases where the patient cannot describe the problems. The issues are often associated with cognitive disabilities, such as lack of feeding or inactivity. [4][16][17]

Alzheimer's disease symptoms are very similar to those of some physical ailments, and many symptoms appear in phases. Each ailment requires a different diagnosis; none of the estimation methods available today can cope with these distinguishing attributes. However, patients can be misdiagnosed with severe health issues. Generally, patients who receive a diagnosis at earlier stages of the disease can be cared for by their families to avoid medical care services; therefore, the family would rather prioritize the health of the patient. Early diagnosis of Alzheimer's disease will assist

physicians in initiating the appropriate medications tailored for the treatment phase of Alzheimer's disease as soon as possible. [4][6] [18][6]

Automatic Speech Recognition (ASR) involves converting spoken words to text. ASR systems may include mechanisms for transcribing natural speech, where words are converted into corresponding text, although these are usually developed with a specific application domain in mind. Some of these systems require continuous speech, while others require speech pruning (periods of silence) between each spoken word to facilitate the understanding of the system. The detection of these speech prunings in a continuous speech interval requires the use of algorithms that are able to detect this event in an energy decomposition, e.g., silence or voice activity detection, which can use energy threshold or Mel-frequency cepstral coefficients. These can easily be accessed in computer libraries [19-21].

However, specific neural networks have already been created specifically for speech recognition that, unlike VADs, carry out the entire process from sound to written word. These deep learning-based models aim to perform various kinds of detection, including vocabulary and text-level word alignments, as well as phoneme-level information, phone duration, etc. Some of them use large monophony datasets and switchboard corpora, allowing a good probabilistic output on various sentences, which may contain words inherent to a specialized vocabulary [22]. These models use narrow-band noise suppression, beamforming, acoustic model preprocessing with deep learning, decoding, and end-point detection to generate hypotheses for words related to the model's vocabulary. These hypotheses are generated probabilistically, and the output of all of them is evaluated by a hidden Markov model algorithm, aiming to convert the hypotheses into written text with a high chance of success [23].

5. The proposed RFC-LSTM Model

Many recent studies have shown that long short-term memory models are effective in a wide range of natural language processing applications. In deep learning models, the ability of the algorithm to learn from more data can be crucial to its performance. In RNN and LSTM models, some mini-batch methods help take advantage of parallelism. The LSTM model learns better and faster with sequence data when prediction decisions are quicker. However, this method also has its pitfalls, as it can limit performance improvement. The problem is storage capacity; the data length that can be learned depends on the available data capacity, so it is important to use the available capacity effectively. LSTM models with traditional techniques do not effectively and efficiently use the information of each variable. To this end, a method called Random Forest Clustering LSTM is proposed and evaluated in the first place with theoretical foundations, and then the algorithmic model is substantially proposed. [4][19][6]

6. Alzheimer's Disease Prediction Model

One of the most important applications of predictive analytics today, particularly in the field of bioinformatics and biomedicine, is predicting the diagnosis of healthcare problems of positive patients as accurately as possible using the algorithms designed by determining different factors that could improve the performance of the models used. With healthcare data, treatment could be started before it is too late. Early diagnosis and prediction in bioinformatics and biomedicine have gained importance in predicting whether some diseases, particularly brain-based ones such as Alzheimer's disease. It aims to predict Alzheimer's disease in the early stage using deep learning techniques and the best features of the brain graph using different feature selection methods. In this study, a hybrid model is proposed based on Recursive Feature Elimination in combination with RF and LSTM algorithms to predict Alzheimer's disease in the mild cognitive impairment stage. The features of the brain graph of the dataset were obtained from three different feature extraction methods, and the best features of the combination of RFE-RF-LSTM were identified using three different feature selection methods. The performances of the model-based accuracy, sensitivity, specificity, and F1-score metrics are calculated and compared. A model for early prediction of the disease is also discussed. In the end, it is aimed to identify the best number of RFE and to determine the optimal number of neurons using three feature selection methods and implement the model at the best number for all six different datasets.

7. Results

Finally, the proposed model was implemented using a workstation with an Intel CPU, 64 GB RAM, and NVIDIA. The evaluation metrics of the model were presented. The weighted average was taken as the final performance measure. The proposed model achieved high predictive performance with an accuracy of 88.3%, precision of 93.5%, F1 score

of 90.4%, and recall of 88.3%. However, it showed less performance in terms of AUC. Graphically, the model performed better, taking values close to 1. Lastly, comparison analysis was performed using various tools. AUC-ROC is a commonly employed statistical analysis, and the comparison was conducted based on AUC-ROC. However, AUC-ROC is non-informative when determining the classification problem. In such cases, the precision-recall curve was applied.

The precision-recall curve showed that the proposed model had high predictive performance. The proposed model was superior to other models through the precision-recall curve. Concerning the previous study, the proposed model showed superior performance; however, performance risks were apparent in the final stage of evaluation. The final stage comprising weak points was the limitation of the commercial database, specifically in terms of the imbalanced distribution of datasets. The imbalanced data distribution decreases the performance of the model, particularly in predicting the minority class. After training, the model showed less performance in the evaluation.

8. Discussions

Early prediction of Alzheimer's disease depends mainly on the identification of patients with mild cognitive impairment (MCI), which affects elderly individuals, as it might eventually progress to this severe neurological disorder. This paper has highlighted the treatment and handling of the MCI progression dataset, where thresholding gives more than twofold accuracy over a sequence length of only six epochs for tasked age prediction. This is achievable through the combination of proper feature extraction, namely a learned convolutional scale of multiresolution transmission; an efficient classification model based on the random forests classifier; and the bi-directional long short-term memory for temporal dependencies. Finally, it is also worth noting that it is not computationally heavy, which is crucial when it comes to healthcare applications.

Although the vast majority of the provided solutions for early Alzheimer’s disease prediction are mainly deep learning-based, in this paper we elected to put full effort and interesting contributions to the prospect of alleviating the computational issue while achieving high accuracy. A good identification of the conditions might help in delaying the manifestation and consequently improving the quality of life.

9. Conclusion and Future Works

We made a prediction on Alzheimer’s disease using the RFC or LSTM model, which gave good and satisfying results. Then, we tried both RFC and LSTM with a single approach and combined both using ensemble methods with LSTM and RFC together. The result of the latter was a little bit disappointing. Using RFC or LSTM only also gives a satisfying result. In a single approach, using RF instead of RFT is recommended because the accuracy is a little bit disappointing, along with other performance metrics. LSTM works better. We have min-max normalized the input and output. Dropout for LSTM is not recommended. Then, the next step is to do dimensionality reduction using feature selection or clustering. It gives a satisfying result but needs more experimentation. In the future, deeper research can also address the importance of clinical factors. The RFC-LSTM model can also be enhanced by various approaches in the LSTM model. Currently, from observation, the data representation and learning through random classifiers can be further enhanced.

References

[1] S. P. Haen, M. W. Löffler, H. G. Rammensee, "Towards new horizons: characterization, classification and implications of the tumour antigenic repertoire," *Nature Reviews Clinical*, 2020. nature.com

[2] M. Agostini, G. Benato, J. A. Detwiler, and J. Menéndez, "Toward the discovery of matter creation with neutrinoless decay," *Reviews of Modern Physics*, 2023. aps.org

[3] A. J. Kerr, D. Dodwell, P. McGale, F. Holt, and F. Duane, "Adjuvant and neoadjuvant breast cancer treatments: A systematic review of their effects on mortality," Cancer treatment, Elsevier, 2022. sciencedirect.com

[4] A. A. Tahami Monfared, M. J. Byrnes, and L. A. White, "Alzheimer's disease: epidemiology and clinical progression," Neurology and ..., 2022. springer.com

[5] J. Fortea, S. H. Zaman, S. Hartley, M. S. Rafii, "Alzheimer's disease associated with Down syndrome: a genetic form of dementia," The Lancet, 2021. escholarship.org

[6] C. S. Liang, D. J. Li, F. C. Yang, and P. T. Tseng, "Mortality rates in Alzheimer's disease and non-Alzheimer's dementias: a systematic review and meta-analysis," The Lancet Healthy, 2021. thelancet.com

[7] C. A. Papanastasiou, C. A. Theochari, "Atrial fibrillation is associated with cognitive impairment, all-cause dementia, vascular dementia, and Alzheimer's disease: a systematic review and meta-analysis," *Journal of General*, 2021. springer.com

[8] J. A. Flores-Cordero, A. Pérez-Pérez, "Obesity as a risk factor for dementia and Alzheimer's disease: the role of leptin," International Journal of…, 2022. mdpi.com

[9] P. Iso-Markku, U. M. Kujala, K. Knittle, and J. Polet, "… as a protective factor for dementia and Alzheimer's disease: systematic review, meta-analysis and quality assessment of cohort and case–control studies," British Journal of Sports Medicine, 2022. bmj.com

[10] R. S. Turner, T. Stubbs, D. A. Davies, and B. C. Albensi, "Potential new approaches for diagnosis of Alzheimer's disease and related dementias," Frontiers in neurology, 2020. frontiersin.org

[11] A. Avan and V. Hachinski, "Stroke and dementia, leading causes of neurological disability and death, potential for prevention," Alzheimer's & Dementia, 2021. [HTML]

[12] G. C. N. Wong and K. H. M. Chow, "DNA damage response-associated cell cycle re-entry and neuronal senescence in brain aging and Alzheimer's disease," Journal of Alzheimer's Disease, 2023. sagepub.com

[13] MK Singh, Y. Shin, S. Ju, S. Han, and S. S. Kim, "Comprehensive Overview of Alzheimer's Disease: Etiological Insights and Degradation Strategies," *International Journal of*, 2024. mdpi.com

[14] R. Sanchez-Varo, M. Mejias-Ortega, "Transgenic mouse models of Alzheimer's disease: An integrative analysis," International Journal of ..., 2022. mdpi.com

[15] B. Kim, G. O. Noh, and K. Kim, "Behavioural and psychological symptoms of dementia in patients with Alzheimer's disease and family caregiver burden: a path analysis," BMC geriatrics, 2021. springer.com

[16] W. M. van der Flier, M. E. de Vugt, E. M. A. Smets, and M. Blom, "Towards a future where Alzheimer's disease pathology is stopped before the onset of dementia," Nature Aging, 2023. nature.com

[17] X. Li, X. Feng, X. Sun, N. Hou, and F. Han, "Global, regional, and national burden of Alzheimer's disease and other dementias, 1990–2019," Frontiers in Aging, 2022. frontiersin.org

[18] A. Sundström, A. N. Adolfsson, M. Nordin, "Loneliness increases the risk of all-cause dementia and Alzheimer's disease," The Journals of ..., 2020. oup.com

[19] Z. Breijyeh and R. Karaman, "Comprehensive review on Alzheimer's disease: causes and treatment," Molecules, 2020. mdpi.com

Kerbala Journal of Computing and Technology 2025

Text Steganography in Videos Using Ascii Code Values

Ahmed Mahmoud Hassan[a], Hassan Abdulhadi Fadel[a] ,Mohammed Muntazir Rushdi Belibas[a], Mohammed Jassim Abdul Sada[a] ,

Estqlal Hammad Dhahi[b], Ashwan A. Abdulmunem[a], Zahraa A. Harjan[a]

[a]*Department of Computer Science, College of Computer Science and information Technology, University of Kerbala, Kerbala, Iraq*

[b]*Information Technolog y Centre, University of Kerbala,Kerbala,Iraq*

Received: 17 / 03 /2025
Accepted: 14 / 05 /2025
Published: 30 / 06 / 2025

Keywords:

Steganography, Text steganography, SHA512-ECC , CM-CSA

ABSTRACT

Text steganography is a technique used in digital video files to conceal text. Sensitive information, such passwords or messages from outside parties, has long been hidden using this method. Depending on the user's intention, text steganography can be used for both good and bad things. The procedure is adding brief textual captions to each frames in a video file without appreciably altering the film's overall size or look. Next, an algorithm is used to encrypt the embedded data, making it difficult for unauthorized users to access and perhaps intercept the transmission. This technique makes it possible to send encrypted messages securely via networks without being discovered by outsiders trying to obtain private data that is hidden in videos that they are not allowed to watch. Through digital media platforms like YouTube or Video, text steganography offers businesses and individuals alike an efficient method to safeguard their data while still securely sharing it with others. Because only people with the ability to decode secret texts will be able to access them once they are embedded into a video file format, it also gives them more control over the kind of content they publish online. In this paper a new approach for hiding ASCII code values in videos has been tested and evaluated which presents an acceptable result in this field.

1. Introduction

Nowadays, protecting data from an unauthorized user is the primary task of transmitting information over a communications network. To deal with this issue there are various mechanisms such as Steganography, Cryptography, Digital Watermarking, etc. The first two methods provide protection on the data, while the third method provides authentication of the data by using some tags or marking some objects such as text, audio, video, and image. Steganography is a powerful technology used in information security. Encryption was initially developed and used as a method of securing the confidentiality of information. But keeping the message's contents confidential is sometimes not enough. It may also be necessary to keep the message's existence secret and the concept responsible for this is Steganography. The word Steganography has a Greek origin and means hidden writing from the Greek words stegao meaning covered or protected, and graph in meaning writing. Hiding information is a way to hide confidential messages within any media. Which are categorized into hiding pictures, text, audio and video, and which are based on the cover media used to embed a confidential message. Most data masking systems take advantage of human perceptual weaknesses. The science of steganography is often confused with encryption because the two are

∗Corresponding Author: Hassan, Ahmed

Email addresses: m05141150@s.uokerbala.edu.iq

similar in the way they are used to protect confidential information. If both methods are used: encryption and concealment of information, the connection becomes double secure. The main difference between Steganography and cryptography is that cryptography focuses on preserving the confidentiality of the message contents while cryptography focuses on preserving the confidentiality of the message's existence. There are many works in steganography which applied on visual data. In this work we proposed a method based on ascii code to hide information "text" in video frames following sections will explain it in details.

2. Related Works

To get and hide the information in the video, a combination of cryptography and steganography using SHA512-ECC and CM-CSA was presented. Initially, ordinary text is used as an input, and it is subjected to IHE pressure and DNA encoding. The results showed that the suggested CM-CSA algorithm is superior than the SHA512-ECC technique for cover media steganography[1].

Steganography it's provided techniques by using the Zero Distortion Technique it's depending on the location of the bit is applied on gray as well as color image, in the color image can hide more data comparing with gray because color image contains RGB bands[2]. Another technology of steganography using (ACA) ant colony algorithm and LSB, this algorithm has shown to be exceptionally effective in producing the secret key by arriving at feeble pixels haphazardly [3].

It analyzes the LSB (least significant bit) to other popular methods. Generalized Gaussian Distribution (GGD) to identify the presence of hiding information in LSB. In color images, we compared the features of LSB to those of other HCFCOM and HOMMS, and in grayscale images, we compared the features of LSB to those of HCFHOM, HOMMS, A. HCFCOM, and C.A. HCFCOM[4].by utilizing the Least Significant Bit (LSB) procedure an Adaptive Random Inverted Pattern (ARIP) approach has endeavored to additional upgrade the nature of the stego-image. comparing the MSE and PSNR values of the image ensures the (PSNR) Peak Signal to Noise Ratio increasing for the ARIP technique yields 1 dB improvement [5]

Based on the Chinese remainder theorem (CRT) it suggests a new schema called (SIS) Secret image sharing to use steganography and it relies upon the number of pixels in the image. The schema can accomplish both the high PSNRs of the stego image. SIS extended to RESIS and the outcome proved the RESIS better than SIS, the outcome proves the schema is better existing methods [6]. While utilizing threshold PRASIS schema-based SIS under G F (28) into the AMBTC cover picture. the result its be good effectiveness and high accuracy [7]

A new text steganography method was proposed as an approach. The method involves mixing the ASCII value of a character with the RGB values of a pixel to store an individual character in a single pixel. The fundamental goal of this method is to give the highest possible payload capacity for an image, which is the total amount of pixels it includes [8]. This method was based on two basic concepts: (1) recognizing highly dynamic regions in video scenes and using them to hide data, and (2) finding the appropriate quantity of data to embed in the selected regions. The dynamics of the scenes were studied using motion hints from feature points, and then the regions of interest were chosen accordingly. The average embedding capacity and perceptual invisibility rate values obtained in the experiments are 0.52 bpp and 50.66 dB, respectively [9].

Proposed a new video data hiding approach that takes advantage of the capacity of repeat accumulate codes to remedy errors as well as the superiority of forbidden zone data hiding (FZDH). FZDH was used to ensure that no changes are made to the data while it is being hidden [10]. On text, image, audio, and video as a media, they covered the numerous forms and approaches of steganography [11][12]. They were discussing Some of the techniques of text steganography has been discussed along with characteristics and working.

A research work presented that looked at three approaches based on least significant bit (LSB) algorithms. They provided a new method for LSB-based image steganography. Reduce the length of the secret message using the Deflate method, which combines the LZ77 and Huffman algorithms to provide a lossless data compression algorithm. The AES (Advanced Encryption Standard) algorithm was used to safeguard the decreased hidden data [13].

Another work proposed steganography technique based on Optical Character Recognition (OCR), where in the cover of the image the message was embedded. There from images character level features extracted which contain the

textual message, and in the cover, image embed these features. the results was validated on an English Printed Character dataset (Chars74K Dataset) [14]. In the edge of the frames of the AVI video, the secret message (English text) was hidden, without changing the details of frames. In the frames 38,39,40,41 and 42 the secret message was embedded because these frames have sufficient edge point details the reason of selecting those frames. the secret message has been represented with a message comprised of 300 characters, and the cover frame image is represented by a 120 frames size 120* 160.The results obtained the Peak Signal to Noise Ratio (PSNR) value ranges from 74.5293dB to 75.9123 dB [15].

The method used was ASCII coding to hiding the secret message, if someone understands its applicability the CASE method has a security issue that, so it is easy to attack. To overcome its limitations the DSTS algorithm is applied by using UTF-16 coding and the security of CASE is enhances with a one-time pad (OTP) which is a theoretically unbreakable cryptographic method. The average hiding capacity was degrades in a PHM from 2.06% to 1% due to UTF-16 coding. The MDSTS and the CMPHM is improved by 6.49% and 7.76% hiding capacity [16].

There were those who suggested relying on the use GA to protect stego text from suspicion due to the efficiency and effectiveness used in other media. To avoid third parties detecting the existence of secret message therefore Suspiciousness against stego text is very important in steganography [17].

Text-based steganography methods could be employed in Web page texts as well as plain text. The ability to broadcast messages (e.g., HTML codes and Hashtags on social media) was the same whether hidden information is there or not. The secret message was hidden in the content or the code of a Web page by using its properties. To improve the security of Persian messages sent across networks, certain text steganography methods were proposed [18].

To improve the capacity of hidden data in social media communications. An approach was devised in which any simple piece of text, such as a news item, a letter, or common messages, was used as the cover text. Extended Line will be used to enhance the capacity of a text, followed by White Space between lines [19].

By taking into account good visual quality, some had suggested a way to improve the LSB technique's capacity. Rather of replacing LSB with secret data, the secret data was used for embedding. First, the minimum and maximum values in the secret data are calculated, and then all values in the secret data are subtracted from this maximum value. Finally, after creating a division for the results, insert the new results into the cover image to obtain the stego image. When compared to earlier approaches, the end outcome was good but unnoticeable [20].

There were those who used a technique to hide secret data in the media cover. In order to get an optimum position to hide the data the GA is Applied to the audio samples of cover file encoded the secret data into its ASCII, finally to secret data LSB is used to embed the ASCII codes [21]. A number of researchers presented an overview of the existing techniques for hiding text and its classifications, and a comparison between these techniques, looking at the use of text document in organizations on a large scale, using text document as a cover medium might be a best choice in such environment [22].

To hide secret messages in a video, use Discrete Wavelet Transform (DWT) and Advanced Encryption Standard (AES). AES used to be message encrypted more secure. From the experiments the value ranges from 39 to 40 dB of PSNR value and close to 1 of SSIM value, which means does not cause large noise due to insertion [23]. There are a number of researchers who have presented a comprehensive study of the methods of modern text steganography and their classification. Among the researchers, the methods of hiding text are divided into three categories: linguistics methods, random and statistical generation, and format-based [24].

When the hiding uses encryption and steganography techniques to provide greater protection for data sent over insecure channels. The encryption method based on the genetic algorithm gave good results, which increased the strength of the encryption, as unauthorized people could not know the key without knowing the random seeds that generated using this algorithm. The embedding of even and single-layer frames also makes the video look natural and uninterrupted. The experimental results of this method showed that the inclusion was of high quality and the metric

values were close to the ideal value. This indicates that this method fulfills the lack of feeling of the inclusion in the video. In the end, the results provide a high capacity, which the result PSNR is 63 [25].

3. Proposed Method

Because video streams have a significant degree of spatial and temporal redundancy in representation and have extensive uses in daily life, they are thought to be suitable candidates for hiding data. Video steganography can then be used in a variety of practical applications. One use is for military and intelligence services to employ video steganography in their communications. Another use is to employ video steganography to send supplementary data, such as subtitles.In general, video steganography is an extension of visual steganography. A video file can be seen as a series of photos, resulting in video data hiding that is comparable to image data hiding.

However, there are several distinctions between video steganography and picture steganography. Because video material is dynamic, the odds of detecting concealed data are smaller than with photos. In addition to picture attacks that may be applied to individual frames of video, there are many additional video assaults such as lossy compression, altering the frame rate, switching between formats, and adding or deleting frames during video processing. Furthermore, the concealing capacity of video is substantially larger. Videos add new aspects to data concealment, such as hiding messages in motion components.

The proposed approach uses the RGB values to embed a single character. At the beginning it takes the first character of the message and divides its ASCII value into three segments, for instance if the character is “A” then its ASCII value would be “65” and after dividing the value into three segments the three numbers would be “0”,”6”, and “5” The three values then embedded in the RGB values of each pixel. Then combine these three numbers into a single pixel using its three channels (Red, Green and blue). Fig. 1. explains the method.

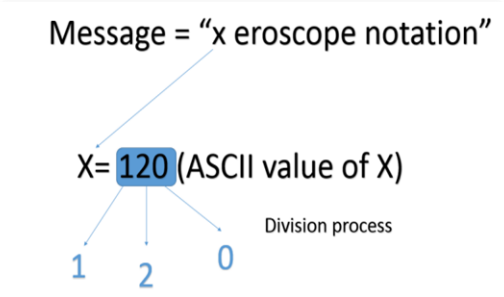


Fig. 1- Steganography Based on ASCII Code

Algorithm for the embedding process:

- Read the message to be embedded.
- Decode the characters to their corresponding ASCII values.
- Loop through the video frames.
- For each frame do the following:
    - Loop through the frame.
    - Apply division on the ASCII value to get the three numbers.
    - Embed the three values in the pixel.
    - Repeat until the end of the frame.
- Add end point.

Algorithm for the extracting process:

- Read the video.
- Loop through the video frames.
- For each frame do the following:
    - Loop through the frame.
    - Get the values of Red, Green and Blue from each pixel.
    - Extract the last digits from Red, Green and blue.
    - Combine the values to obtain the ASCII value.
    - Repeat until the end of message point reached.

The approach yields very good results, since in the worst-case scenario the difference in intensity would be only 9 points and that is entirely unnoticeable by the naked eye, however, an important point should be mentioned is that there is an exceptional case in this approach which can occur when the resulting channel value exceeds 255 (which is the highest value for any given channel in the pixel), for instance if the data to be embedded is 119 (which corresponds to the letter 'w') and the original pixel value is:

R = 19, G = 19, B = 251

And after embedding we get the following values:

R = 11, G = 11, B = 259

Notice that the Blue channel value has exceeded the one-byte value limit. We worked around this exceptional issue by skipping the problematic pixel, we established that by embedding a non-printable control character such as the SOH character (Decimal 1) provided that the same would be done when extracting.

4. Results and Discussions

The suggested method was tested on multiple videos with various sizes and various messages. The messages sizes varied from small messages to extremely huge (e.g. more than 5 million characters) and contained all printable ASCII characters. Steganography efficiency was tested with PSNR (peek signal to noise ratio) which is a common measure to test similarity between frames. In the experiments we used three MP4 videos and two large messages one is the whole works of Shakespeare with more than 5 million characters and the other is the very famous novel by Leo Tolstoy "War and peace" with more than 3 million characters. Table 1 shows the videos that have been used in the experiments.

Table 1 - Test Cases Video Information

Test Cases	Frame Rate	First Frame from Videos
Video #1	29	
Video #2	23	
Video #3	23	

5. Experimental Results

The following table explains the characteristics of the video that used to hide the text. Table 3 depicts the PSNR for video #1. While table 4 show the information of the video after stegonagraphy process.

Table 2- Video Information

Size	Number of Frames Needed	Average PSNR
461 MB	25	35.3122

Table 3- PSNR for Test Video 1

Frame NO.	PSNR value
1	35.1014
2	35.1213
3	35.1168
4	35.1188
5	35.1276
6	35.1132
7	35.1120
8	35.1106
9	35.1095

10	35.1095
11	35.0992
12	35.1258

Table 4-Video Information After Steganography Process

Width	Height	Frame rate	Duration	Original size	Payload length
640	360	29	23 S	1.7 MB	5,583,449 characters

Table 5- Methods Comparisons

Technique	Methods	Embedding techniques	Advantages	Drawbacks
Temporal Domain	Low bit encoding (least significant bit)	LSB of each audio sample is replaced with data sample	Easy and simple data hiding in target signal	Easy to extract and to destroy
	Echo hiding	Cover data by introducing echo signal in target signal	Resilient to lossy data compression algorithms	Low Capacity and security
Transform Domain	Phase spectrum	Modulate the phase of the cover signal	Robust against signal processing manipulation and data retrieval needs the original	Low capacity
	Magnitude spectrum	Use frequency bands to hide data	Longer message to hide and less likely to be affected by errors during transmission	Low robustness to simple audio manipulations

6. Conclusion

The steganography approach was implemented in this project was originally proposed for images. In this project an extension to the original approach was proposed and implemented to include video files. Testing data showed

excellent results when it comes to payload size and PSNR, with payload size exceeded 5 million characters and average PSNR of (34.942) which is quite decent and unnoticeable by the human eye. However, the only downside for this approach that we could notice was the resulting video size which can be mitigated by using lossless compression.

References

[1] A. Jose and K. Subramaniam, "DNA based SHA512-ECC cryptography and CM-CSA based steganography for data security," Mater. Today Proc., no. xxxx, 2020, doi: 10.1016/j.matpr.2020.09.790.

[2] Shivani, V. K. Yadav, and S. Batham, "A Novel Approach of Bulk Data Hiding using Text Steganography," Procedia Comput. Sci., vol. 57, pp. 1401–1410, 2015, doi: 10.1016/j.procs.2015.07.457.

[3] A. I. Al-Hussein, M. S. Alfaras, and T. A. Kadhim, "Text hiding in an image using least significant bit and ant colony optimization," Mater. Today Proc., no. xxxx, 2021, doi: 10.1016/j.matpr.2021.06.413.

[4] Q. Liu, A. H. Sung, B. Ribeiro, M. Wei, Z. Chen, and J. Xu, "Image complexity and feature mining for steganalysis of least significant bit matching steganography," Inf. Sci. (Ny)., vol. 178, no. 1, pp. 21–36, 2008, doi: 10.1016/j.ins.2007.08.007.

[5] R. Amirtharajan and J. B. Balaguru Rayappan, "An intelligent chaotic embedding approach to enhance stego-image quality," Inf. Sci. (Ny)., vol. 193, pp. 115–124, Jun. 2012, doi: 10.1016/j.ins.2012.01.010.

[6] K. Meng, F. Miao, Y. Xiong, and C. C. Chang, "A reversible extended secret image sharing scheme based on Chinese remainder theorem," Signal Process. Image Commun., vol. 95, Jul. 2021, doi: 10.1016/j.image.2021.116221.

[7] X. Wu and C. N. Yang, "Partial reversible AMBTC-based secret image sharing with steganography," Digit. Signal Process. A Rev. J., vol. 93, pp. 22–33, 2019, doi: 10.1016/j.dsp.2019.06.016.

[8] K. Joshi, "A New Approach of Text Steganography Using ASCII Values." [Online]. Available: www.ijert.org , doi: 10.17577/IJERTV7IS050273.

[9] M. Hashemzadeh, "Hiding information in videos using motion clues of feature points," Comput. Electr. Eng., vol. 68, pp. 14–25, May 2018, doi: 10.1016/j.compeleceng.2018.03.046.

[10] K. Deshpande and N. Kamble, International Journal of Computer Science and Mobile Computing "Application of Data Hiding in Audio-Video Using Advance Algorithm," 2016. [Online]. Available: www.ijcsmc.com , doi: 10.47760/ijcsmc.

[11] A. Febryan, T. W. Purboyo, and R. E. Saputra, "Steganography Methods on Text, Audio, Image and Video: A Survey," 2017. [Online]. Available: http://www.ripublication.com , doi:10.37622/000000.

[12] S. Sharma, A. Gupta, M. C. Trivedi, and V. K. Yadav, "Analysis of different text steganography techniques: A survey," in Proceedings - 2016 2nd International Conference on Computational Intelligence and Communication Technology, CICT 2016, Aug. 2016, pp. 130–133, doi: 10.1109/CICT.2016.34.

[13] S. L. Chikouche, and N.Chikouche. "An improved approach for lsb-based image steganography using AES algorithm." 2017 5th International Conference on Electrical Engineering-Boumerdes (ICEE-B). IEEE, 2017, doi: 10.1109/ICEE-B.2017.8192077.

[14] A. Chatterjee, S. K. Ghosal, and R. Sarkar, "LSB based steganography with OCR: an intelligent amalgamation," Multimed. Tools Appl., vol. 79, no. 17–18, pp. 11747–11765, May 2020, doi: 10.1007/s11042-019-08472-6.

[15] A. M. Aaref, "Video Steganography Using LSB Substitution and Sobel Edge Detection," Diyala J. Eng. Sci., vol. 11, no. 2, pp. 67–73, 2018, doi: 10.26367/DJES/VOL.11/NO.2/9.

[16] Y. Khan, A. Algarni, A. Fayomi, and A. M. Almarashi, "Disbursal of Text Steganography in the Space of Double-Secure Algorithm," Math. Probl. Eng., vol. 2021, 2021, doi: 10.1155/2021/7336474.

[17] B. Osman, A. Yasin, and M. Nizam Omar, "An Analysis of Alphabet-based Techniques in Text Steganography."

[18] S. R. Yaghobi and H. Sajedi, "Text steganography in webometrics," Int. J. Inf. Technol., vol. 13, no. 2, pp. 621–635, Apr. 2021, doi: 10.1007/s41870-020-00572-z.

[19] H. J. Shiu, B. S. Lin, B. S. Lin, P. Y. Huang, C. H. Huang, and C. L. Lei, "Data hiding on social media communications using text steganography," in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2018, vol. 10694 LNCS, pp. 217–224, doi: 10.1007/978-3-319-76687-4_15.

[20] D. Nashat and L. Mamdouh, "An efficient steganographic technique for hiding data," J. Egypt. Math. Soc., vol. 27, no. 1, Dec. 2019, doi: 10.1186/s42787-019-0061-6.

[21] A. Mishra , P.Johri , A . Mishra. "Audio steganography using ASCII code and GA." 2017 International Conference on Infocom Technologies and Unmanned Systems (Trends and Future Directions) (ICTUS). IEEE, 2017,doi :10.1109/ICTUS.2017.8286088.

[22] R.Bala Krishnan1, Prasanth Kumar Thandra , M.Sai Baba "An overview of text steganography." 2017 Fourth International Conference on Signal Processing, Communication and Networking (ICSCN). IEEE, 2017,doi :109/ICSCN.2017.8085643 .

[23] M. Mulya, O. Arsalan, L. Alhaura, R. Wijaya, S. Ramadhan, and C. Yeremia, "Text Steganography on Digital Video Using Discrete Wavelet Transform and Cryptographic Advanced Encryption Standard Algorithm" Advances in Intelligent Systems Research, volume 172, Sriwijaya International Conference on Information Technology and Its Applications (SICONIAN 2019), doi :10.2991/aisr.k.200424.021.

[24] M. A. Majeed, R. Sulaiman, Z. Shukur, and M. K. Hasan, "A review on text steganography techniques," Mathematics, vol. 9, no. 21. MDPI, Nov. 01, 2021, doi: 10.3390/math9212829.

[25] Z. Jasim, M. J. Altalqani, and Z. J. Jaber, "Improving The Security Of Steganography In Video Using Genetic Algorithm Arabic Plagiarism detection system View project Improving The Security Of Steganography In Video Using Genetic Algorithm," 2021. [Online]. Available: https://www.researchgate.net/publication/357889185,doi : 10.17762/turcomat.v12i10.5265.