Journal of Advanced Zoology

ISSN: 0253-7214
*Volume **44** Issue **S-6 Year 2023** Page **575:582***

Enhancing Security Authentication of Information System using Morse code and Facial Recognition

Tejas Purvimath*, Ashwinkumar U M, Tejus Khadri

[1,2,3]*School of Computer Science and Engineering, REVA University, Bengaluru, India*
tejaspurvimath13@gmail.com
tejuskhadri@gmail.com
ashwinkumar.um@reva.edu.in

**Corresponding author's E-mail: tejaspurvimath13@gmail.com*

Article History

Received: 06 June 2023
Revised: 05 Sept 2023
Accepted: 29 Nov 2023

Abstract

Information Technology Management is combination of Data Exchange, Algorithm Development, and implementation of various technologies in order to solve the problems related to Information System security. The applications of data science are used by almost all Information Systems in various domains like educational institutions, finance, healthcare, business to handle large volumes of data. The practical applications range from predicting stock movement to predicting cancer. It is used in image processing to identity recognition, audio processing for speech to text prediction. Since authentication and security of the Information System are still not completely secure and is a matter of concern, we are able to implement a real time eye-tracing along with the facial feature recognition using Morse Code based secured authentication system to enhance the Security aspects of the Information Systems. Most of the traditional Information Systems have a single layer of security authentication and cannot be relied upon. In our findings, we do not find the existing systems to be completely secure and hence we focus on implementing multiple layers of unique security authentications using eyeball movements to form a distinct Morse Code and the facial feature recognition.

Keywords: *Eye Tracing, Facial Recognition, Morse code, Information System, Security Authentication*

1. Introduction

The Security and privacy of information systems is a very complex and interesting domain, and it is also a matter of concern. So, in this research work in order to address this issue we are developing an authentication system that enhances the security of the traditional information systems. We are implementing a system where morse code is entered through eye blink and in addition to this facial feature recognition is also used. Morse code is a method that is used widely in different domains to cipher and decipher a normal text into sequence of dots and dashes. In addition to the morse code we have also implemented facial feature recognition which finds series of points on the face, such as corners of the mouth, corners of eyes, the silhouette of the jaws to recognize the face. In this paper, we have introduced a validation framework that can be carried out in different areas like banking, medical services, Intelligence organization and so forth where security and protection come into the picture. It also provides a platform for the physically challenged people to access their information systems securely. In the following sections of the paper, we will examine the authentication system which uses eye blink to form morse code and facial feature recognition to recognize the face.

Ease of use

In this paper, we propose a system that consists of a user interface and a back-end database. GUI is created such that the user can interact with the system. In the frontend firstly the user needs to register by providing a username of choice, a password (PIN), and a security keyword. This would be the first layer of registration for morse code-based authentication. The second layer of security authentication will prompt the users to enter the user id of their choice and their username again. This will complete the registration process by capturing the facial feature through the web camera.

After registration, the facial features of the users will be recognized. After which, the user can log in by using the credentials i.e., user id and password. With the help of a web camera, the PIN is taken as an input in the form of Morse code. In the backend, the entered PIN is checked with the stored PIN which was entered into the database by the user while registering. If the entered PIN is not correct, it exits the screen. If the entered PIN is correct, it displays successful authentication. If the user has forgotten his password, then he can use the mouse to click on the hyperlink to authenticate and update the existing password with a new one.

Related work

The problem associated with the traditional Information Systems is that they mostly have a single layer of security authentication that is traditional text-based password, and they are vulnerable to cyber-attacks like shoulder surfing, keylogging, etc. The traditional systems do not use any unique properties of an entity. Even though the Morse Code, Facial feature recognition and eye blinker algorithms are available they have not been integrated so that the security of the information system would be enhanced. In this section, we give a brief introduction to the related work on these tasks.

A. Morse Code detection

In this paper, it was demonstrated that a model of transmitting Morse code can be done through the keyboard via DB9 connector. This encodes the alphabets using a PIC microcontroller and displays the transmitted and the decoded alphabets on the LCD screen. Here, they have used the microcontroller and have developed a system which receives and reads the Morse code using the transmitter which will be controlled by a microcontroller. The system reads the morse code and displays it on the LCD screen with the help of a DB-9 connector. The system utilizes the PIC microcontroller, which has already been programmed to check for the patterns of dots and dashes [2]. This paper proposed a unified neural network called MorseNet which basically detected and recognized morse code in spectrograms. This system used the DL-based architecture to detect and recognize morse code simultaneously [1].

B. Facial Feature Recognition

This paper had proposed a system called driver drowsiness detection system which can be placed inside a vehicle. They have proposed a method to exploit facial landmark detection model for localization of the eyes and its contours. This system uses dlib library which is a machine learning toolkit and OpenCV with python. Facial landmark detection is generally used to detect and recognize human facial features like Nose, Eyes, Jawline, Eyebrows, Mouth. Facial landmark detection is currently applied for head pose estimation, face alignment and swapping, blink detection and more [5]. In this paper, authors had proposed a method which dealt with the frontal face images by using a modified Haar cascade algorithm. By using this algorithm, the authors could detect the image as well as the coordinates. The main attraction of this paper was that they were able to solve different types of images having one object, two objects, and three objects which was not solved previously by any of the existing methods. This system was able to solve this problem by using modified Haar cascade algorithm [6].

C. Eye Blink

In this paper, we came across a system which proposed an authentication process which used gaze-based PIN entry. In particular, this system detected and tracked eye for real time PIN identification using web camera. This system had enabled user to leave no footprints behind or to be safe from shoulder surfing and keylogging attacks and offered a secured authentication system [3]. This paper had proposed a system to help people with motor neuron disease which used eye blink to communicate with others. Eye blinks were converted into morse code and were represented in the form of dots and dashes [4].

As can be seen, the Morse Code, Facial feature recognition and the eye blinker algorithms are available they have not been used in a single application or it has not been integrated into a single system. Thus, in this article, we have developed a system which would integrate all the above features to enhance the authentication of information systems.

2. Materials And Methods

Main Scope of this paper is to explain as how to avoid frauds that occur in various domains like banking sectors, intelligence agencies and healthcare institutions. Eye trackers provide better security compared to any biometric authentication. Eye trackers are the instruments that measure the visual activities. This makes it possible for physically disabled users to interact with computers using their eyes. Our main motivation is to provide secured authentication process which can be implemented in various domains and also help those who are physically challenged.

A. System Architecture

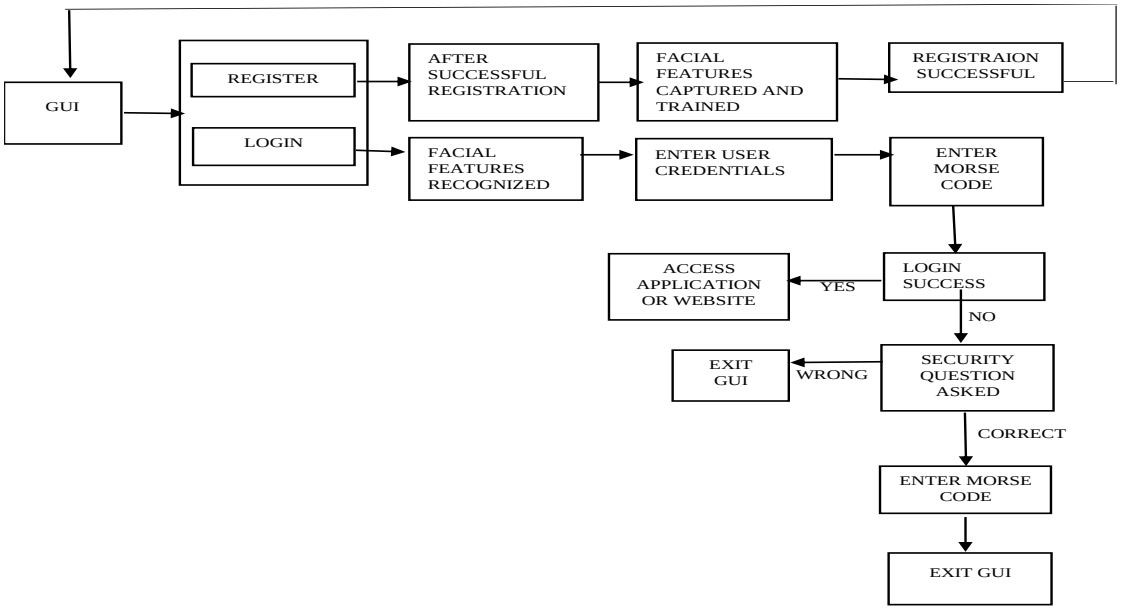

Fig. 1. System Architecure

In the above figure, the architecture of the system has been depicted. It consists of a user interface and back-end database. Graphical user interface is created such that the user can interact with the system. Initially, the user needs to register by providing a user name of their choice, a password (PIN) which would be coverted into morse code while logging in and finally the user needs to enter a security keyword which would come into picture when the user can't remeber their password. The second layer of security authentication will prompt the users to enter the user id of their choice and their username again. This will complete the registration process by capturing the facial feature through the web camera.

After registration, the facial features of the users will be recognized and this is what we consider as the first layer of authentication. After which, the user can log in by using the credentials i.e., user id and password. With the help of a web camera, the PIN is taken as an input in the form of Morse code and in the backend, the entered PIN is checked with the stored PIN which was entered into the database by the user while registering. If the entered PIN is not correct, it exits the screen. If the entered PIN is correct, it displays successful authentication. If the user has forgotten his password then he can use the mouse click on the hyperlink to authenticate and update the existing password with a new one.

B. System Implementation

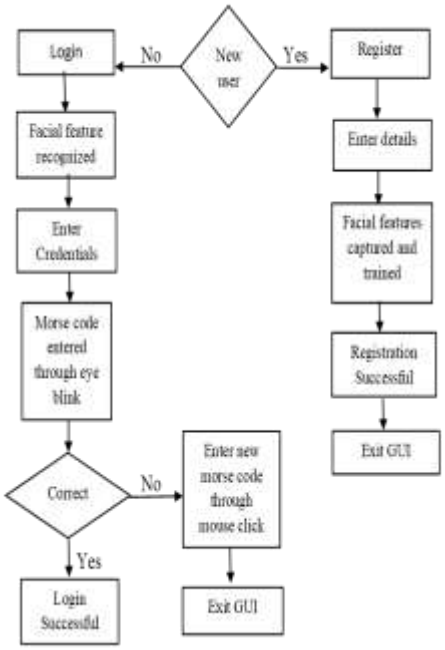

Fig. 2. Implementaion of the mode

When the user firsts open the system Graphical User Interface will prompt the user whether he wants to login or register as a new user. When the user registers, they need to provide the required credentials such as username, password and security keyword. The inputs are stored in a database. When to user needs to login then they must enter the correct credentials which they had given while registering. If the credentials match the ones which were given when they had registered, then the authentication is successful. If the credentials are not matching, then they must answer the security question with the keyword which they had given when they had registered at the beginning. If the keyword matches, then the user can update the password using the mouse click. The updated password is changed in the database. Hence the next time the user logs in they can use the new password which they had set. In a scenario where the keyword does not match then the user exits from the GUI.

C. Dataflow of the model

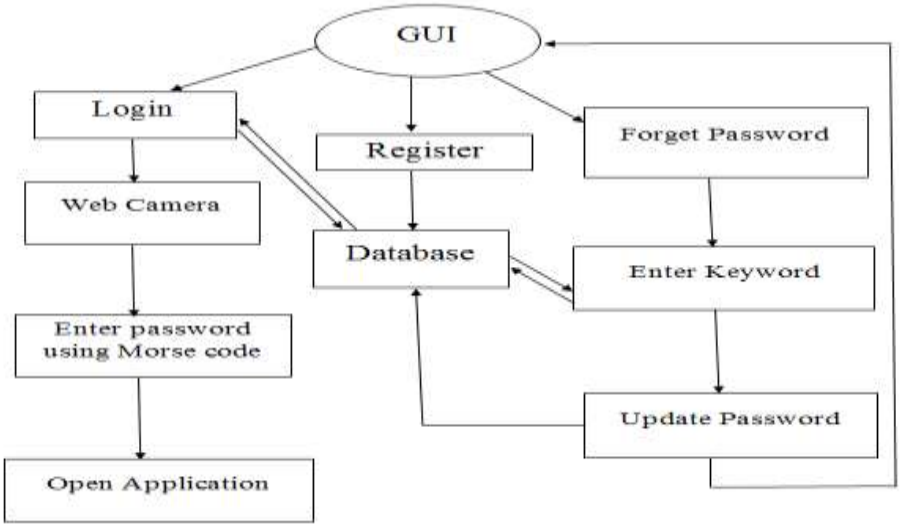

Fig. 3. Dataflow diagram

The above diagram represents the dataflow diagram of our system where the user uses the GUI to register as a new user by providing the required credentials or log in if the user is already an existing user. After registration, the system would enable the web camera to capture the facial features to form a dataset. The dataset is then trained and is associated with the user credentials. In this system, the facial features are detected using Haar Cascade algorithm and facial features are recognized using logical binary pattern histogram algorithm. The eye-tracing is achieved using facial landmark detection algorithm. This database is checked for the user credentials when the user logs into his account to verify whether the user exists or not. The webcam is used to identify the user and takes input of the password

that is entered in the form of Morse code. The webcam converts the blinks generated by the user into Morse code. When the password matches then the required application is opened. In the case wherein the user has forgotten his password then the user needs to answer the security question for which the user had given a keyword at the time of registration. When the keyword is matched with the one in the database then the user can update the password with mouse clicks in the form of Morse code. This change is also updated in the database in real time.

D. Use Case

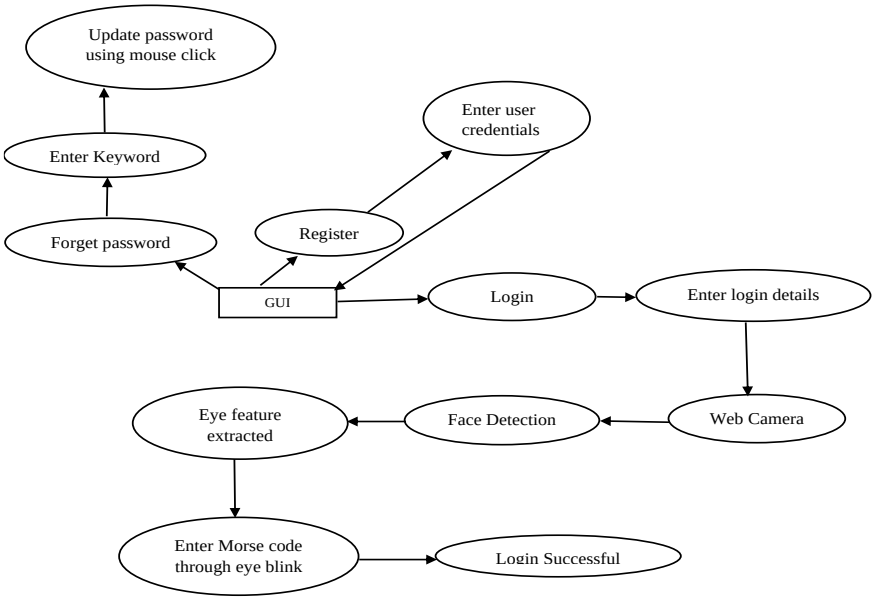

Fig. 4. Use case diagram

The above diagram depicts the Use case diagram for the proposed project. When the user interacts with the GUI (Graphical User Interface) they can login or register themselves as a user. When the user is registering, they need to provide a username, password and a keyword. When the user needs to log in to their account then they need to enter their user id and password. Once they are recognized as genuine users then the web camera is launched. The webcam is used to identify the users face and it begins to extract the features of the eye in real time. During this time, the user needs to enter their password in the form of Morse code by blinking their eyes. If the user can correctly enter the password, then their login is successful. Suppose the user encounters a situation wherein they do not remember their password or wants to change their password then the user needs to answer the security questions with the keyword that they had given when they had registered. When the keyword matches the password can be updated.

E. Sequence Diagram

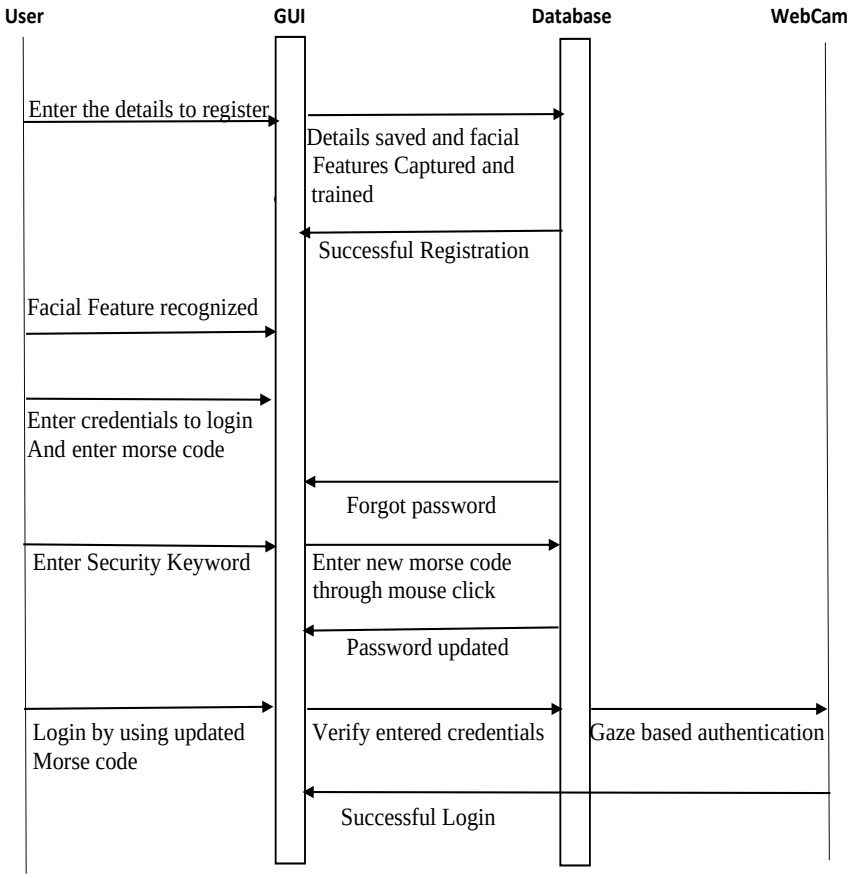

Fig. 5. Sequence Diagram

The above diagram represents the sequence diagram of the model. This diagram consists of three components which are GUI, database and a webcam. The User must perform three actions here. The first action is the registration process, where the user will have to enter the username, password, and security keyword. The communication is between the user and GUI. After a successful registration process, the second action is performed where the user has to login. If the credentials match, then the user can proceed through facial feature recognition and gaze-based authentication. Here the user must blink his eyes to enter the password in morse code. If the user forgets his password, the third action is invoked where the user must create a new password. The new password is created using mouse clicks and this new password would be updated [9-14].

Algorithms

F. Haar Cascade Algorithm

Haar Cascade is one of the machine learning technique where a course work is trained with both positive and negative images. So fundamentally, they are the .xml records with a various feature set. In this section, we will examine how the Haar Cascade classifier functions act as in our framework and how it is utilized to detect a face.

Stage 1: We will import the necessary libraries required such as OpenCV, NumPy and Pandas and direct the location of the stored .xml file.

Stage 2: In this stage, the real time image is converted into greyscale.

Stage 3: After the images are converted into greyscale, the classifier uses the inbuilt function "detectMultiscale" to locate the exact features of the face.

Stage 4: Finally, the inbuilt function "detectMultiScale" would return four different values in the form of dimensions such as x-coordinate, y-coordinate, width and height. Based on these dimensions, a rectangle is formed around the face in order to remove the background from the foreground. Then the features of the face would be detected.

G. Local Binary Patterns Histogram

LBPH is a face recognition algorithm which can represent local facial features in the image. It can recognize both front and the side features of the face. Here, in this segment, we will examine about LBPH Algorithm concerning our authentication system.

Stage 1: Training the Algorithm

At first, we need to train the algorithm in order to recognize the facial features. To do so we need to capture the facial features of the individual that we need to identify. This would be done through the webcam and the image captured is directed to the dataset. We likewise need to enter a name and ID for each picture that is being captured. By doing this we will be providing information required for the algorithm by which it would recognize an input image and give us an output by informing through the user interface that the individual's facial is recognized.

Stage 2: Local Binary Patterns Operation

In this progression, a superior image which describes the original image is created and it highlights the facial features of the captured image. In order to perform this, the algorithm uses parameters like the radius and neighbors.

Stage 3: Extracting Histograms

This step involves the extraction of the Histogram of each regions of the images that were captured in the previous steps.

Stage 4: Face Recognition

At last, the algorithm is completely trained. Each histogram extracted in the previous step is mapped with the images stored in the dataset.

H. Facial Landmark Detection

Face landmark detection is the process of finding points of interest of an image in a human face. In order to accomplish this, the algorithm discovers various focuses on the face like mouth, corners of eyes, the outline of the jaws, and a lot more which will be completed utilizing a trained model function called shape_predictor(). Here, we will examine the facial landmark detector with respect to our security system.

Stage 1: Generally, the pre-trained facial landmark detector is used to detect the location of 68 coordinates. In this authentication system, pre-trained facial landmark detector is used to detect the locations or coordinates of corners of eyes.

Stage 2: Once the coordinates indicating the corners of eyes are detected. Then the coordinates which are recognized around the corners of the eyes are used to enter morse code as a security authentication through eye blinks.

4. Conclusion

The paper basically explains the two-factor authentication system which enhances the security of traditional information system which mostly have single layer of authentication. Two factor authentications are basically providing two layers of security to protect an information system. Here we are making use of facial feature recognition, gaze-based authentication or eye blink and mouse click in order to convert numbers or alphabets into morse code thereby increasing the security. This system can also help people who are physically challenged to authenticate information systems securely. Facial feature recognition in this system can help people who are partially or completely blind to authenticate information systems securely. We truly believe that implementing this system in various domains would enhance the security of the information systems and is the way forward.

Acknowledgment

The finishing of any errand relies on the co-activity, co-appointment and united endeavours of a few assets of learning, vitality and time or more all on appropriate direction. We are thankful to the Director of C&IT School Dr. Sunil Kumar S Manvi for furnishing us with various offices and openings as research centres and types of gear. We owe this snapshot of fulfillment, with a profound feeling of appreciation to our guide Dr. Ashwinkumar U M, for the specialized direction, industrious support, interminable inspiration and everlasting persistence, with whom this undertaking would not be effectively finished. Working under their direction has been devoted and profitable experience. We are genuinely grateful to every one of the individuals from the staff of division of CSE, REVA University and each one of the individuals who have helped us legitimately or in a roundabout way all through the research work.

References:

A. Singh∗ , H, Herunde, F. Furtado, "Modified Haar-Cascade Model for Face Detection Issues" nt. J. Res. Ind. Eng. Vol. 9, No. 2 (2020) 143–171.

Aditya Ranjan, Karan Vyas, Sujay Ghadge, Siddharth Patel, Suvarna Sanjay Pawar, "Driver Drowsiness Detection System Using Computer Vision" IRJET, ISSN: 2395-0056, Volume: 07 Issue: 01 | Jan 2020.

AH Omar Baabood, Prajoona Valsalan, Tariq Ahmed Barham Baomar, IoT Based Health Monitoring System, Journal of Critical Reviews , Vol. 7, Issue. 4, pp. 739-743, 2020.

Bindhia K Francis, Suvanam Sasidhar Babu, Predicting academic performance of students using a hybrid data mining approach, Journal of Medical Systems, 43:162, 2019. https://doi.org/10.1007/s10916-019-1295-4

Jyotsana Raut, Nikita Agashe, Suchita Somkuwar, Trupti Sapate, Pranali Doifode, Ms. Minal Domke, "Morse Passwords Based Authentication System" IJARCET, Volume 3 Issue 3, March 2014

Kavitha H. S., Suguna G. C, "Eye Blink Detection System for Paralyzed Patients" IJRTE, ISSN: 2277-3878, Volume-8 Issue-6, March 2020

Manisha M. Barse, Rodney A. Manual, "Morse Code - A Security Enhancer" IJSETR, ISSN: 2319-7064, Volume 5 Issue 8, August 2016

Mr. Kaustubh S. Sawant1, Mr. Pange P.D, "Real-time Eye Tracking for Password Authentication" IRJET, ISSN: 2395-0056, Volume: 06 Issue: 03 | Mar 2019.

Nikita Raut, Varun Dhuldhoya, "A Review on Various Techniques for Face Detection" IRJET, ISSN: 2395-0056, Volume: 05 Issue: 10 | Oct 2018.

PK Sadineni, Comparative Study on Query Processing and Indexing Techniques in Big Data, 2020 3rd International Conference on Intelligent Sustainable Systems (ICISS), pp. 933-939, 2020.

PM Surendra, S Manimurugan, A New Modified Recurrent Extreme Learning with PSO Machine Based on Feature Fusion with CNN Deep Features for Breast Cancer Detection, Journal of Computational Science and Intelligent Technologies, Vol. 1, Issue. 3, Pp. 15-21, 2020.

Sajay KR, Suvanam Sasidhar Babu, Vijayalakshmi Yellepeddi, Enhancing The Security Of Cloud Data Using Hybrid Encryption Algorithm, Journal of Ambient Intelligence and Humanized Computing, 2019. https://doi.org/10.1007/s12652-019-01403-1

Sudhan Murugan Bhagavathi, Anitha Thavasimuthu, Aruna Murugesan, Charlyn Pushpa Latha George Rajendran, A Vijay, Raja Laxmi, Rajendran Thavasimuthu, Weather forecasting and prediction using hybrid C5.0 machine learning algorithm International Journal of Communication Systems, Vol. 34, Issue. 10, Pp. e4805, 2021.

Weihao Li; Keren Wang; Ling You, "MorseNet: A Unified Neural Network for Morse Detection and Recognition in Spectrogram" IEEE Access, Volume:8, Sept.2020J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73