Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 5, May : 2023

SECURE AUTHENTICATION USING IRIS FACE AND SIGNATURE

1. Mrs.S.Aruna Kumari M-Tech (Ph.D) , Associate Professor, Raghu Institute of Technology (A), email: aruna0454@gmail.com , Visakhapatnam.

2. K.Vivek Nitin Sai Reddy, UG student, Raghu Institute of Technology (A), email: 193J1A0477@raghuinstech.com , Visakhapatnam.

3. K.Venkata Durga Vajubabu, UG student, Raghu Institute of Technology (A), email: 193J1A0473@raghuinstech.com ,Visakhapatnam.

4. N.Dileep, UG student, Raghu Institute of Technology (A), email: 193J1A04A5@raghuinstech.com , Visakhapatnam.

5. K.SaiVarun, UG student, Raghu Institute of Technology (A), email: 203J5A0409@raghuinstech.com , Visakhapatnam.

ABSTRACT: -

System security is becoming increasingly critical. Due to rapid increase in hackers the count of hacked system is increasing so authentication plays a first line of security against hackers. So, by using three security systems like face, iris and signature as a authenticator that enhance the first line of security. It provides one of the most secure authentications. This authentication procedure, which involves in comparing the stored data that is stored in the data base with the person that is scanning near the authenticator then on the background three algorithms will run on the background individually for the face, iris and signature using the convolution neural network if the scanned data matches with the stored data access granted else access denied.

KEYWORDS: -

Convolution Neutral Network, Iris Authentication, Face Authentication, Signature Authentication.

I. INTRODUCTION

Iris Recognition:

Iris recognition is the process of biometric technologies capturing a high-contrast photograph of a person's iris using a infrared light. This process detects the unique patterns in the colored circles of the eyes known as irises, while excluding obstructions like eyelids, eyelashes, and specular reflections. Iris recognition scanners uses infrared light to get the patterns that are not visible to the naked eye, and then convert the image into a set of pixels containing only the iris.

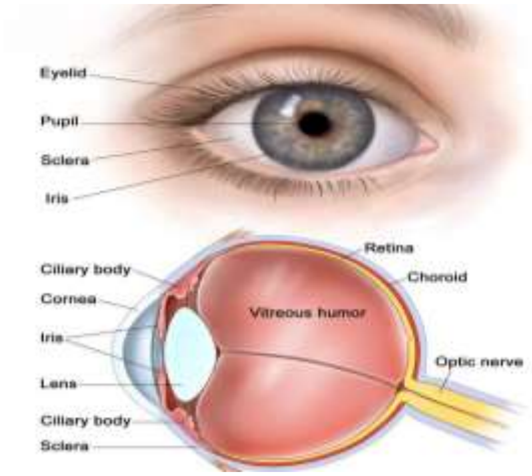


Fig 1. Anatomy of Eye

The next step involves analyzing the patterns of lines and colors in the iris to extract a bit pattern that encodes its unique information. This bit pattern is then digitized and compared to stored templates in a database for verification (one-to-one template matching) or identification (one-to-many template matching).

Face Recognition:

The process of using the individual or person facial features to verify a person's identity is known as face recognition. It is a technology that is used to identify people in photos, videos, and real-time scenarios. Mobile devices are also used by law enforcement to identify individuals during police stops. Face recognition algorithms or software are used by the mobile devices or systems to identify distinct and particular characteristics of an individual's face, such as the spacing between their eyes or the shape of their chin. These details are converted into mathematical representation and then compare given data and the saved face data in the database. The data associated with a particular face is referred to as a face template, which is separate from photograph because it only contains specific details used to differentiate one face from another.

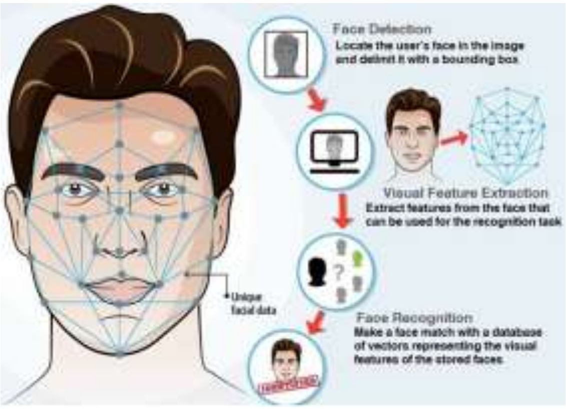

Face Detection
Locate the user's face in the image and delimit it with a bounding box
Visual Feature Extraction
Extract features from the face that can be used for the recognition task
Unique facial data
Face Recognition
Make a face match with a database of vectors representing the visual features of the stored faces

Fig 2. Basic Face Recognition Process

Signature Recognition:

Writing is both a physical expression of human beings and an acquired skill. Signature recognition involves providing a sample of text as a basis for measuring one's writing. The aim of signature recognition is to identify the writer of a given sample, whereas signature verification confirms or rejects the sample. Two distinct techniques are used to analyze writing samples.

The first technique is static and requires the individual to sign their name on paper. The signature is then digitized through an optical scanner or camera, and the resulting data is analyzed through a software algorithm that recognizes the text by analyzing its shape. This is known as an "off-line" mode of recognition. The static, off-line handwriting recognition will be carry out after a text sample has been completed and digitally captured. The captured image data is then converted into a bit pattern which is understandable to software. Off-line signature processing will be having nearly 40 features, including the analysis of the center of gravity, edges, and curves for authentication. However, off-line signature recognition can be challenging due to the normal variability in signatures, the absence of dynamic information on the pen path, and the limited amount of sample data available. Shape matching is mainly used to accomplish the job by identifying and matching key points of the signature to avoid issues with curve detection and parameterization.

The second technique for signature recognition is dynamic. Dynamic signature devices should not be confused with off-line electronic signature capture systems that capture a graphic image of the signature and are common in locations where merchants are capturing signatures for transaction authorizations. Data that is dynamically captured will identify the direction, stroke, pressure, and shape of an individual’s signature which helps to identify the data easily.

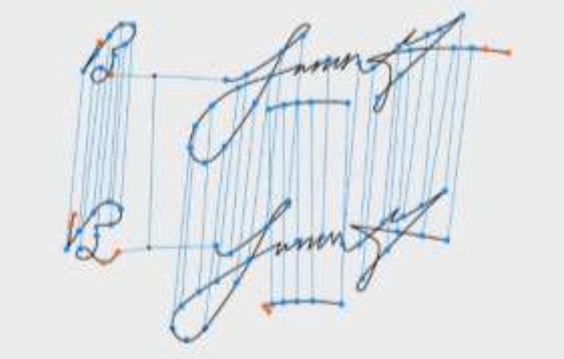


Fig 3. Signature Recognition

II. LITERATURE REVIEW

[1] L. Li, X. Mu, S. Li and H. Peng Face recognition technology is a form of biometric authentication used for identifying an individual's facial features. The process involves collecting images of a person's face, which are then automatically processed by recognition equipment. This paper provides an overview of face recognition research from various perspectives, including its development stages and related technologies. We also discuss the research of face recognition in real-life conditions, as well as the general evaluation standards and databases used in this field. Finally, we offer a forward-looking view of the potential applications and future development of face recognition technology. **[2] K. Kancharla, V. Kamble and M. Kapoor:** Handwritten Signature Recognition is a crucial behavioral biometric that has numerous applications for identification and authentication purposes. There are two methods of signature recognition technique on-line and off-line. On-line recognition is a dynamic approach that utilizes parameters such as writing speed, changes in stylus direction, and the number of pen ups and downs during signature writing. Off-line signature recognition is a static approach in which a signature is treated as an image, and the author of the signature is predicted based on signature features. The current method of off-line signature recognition primarily employs template matching, which compares a test image with multiple specimen images to determine the author of the signature. This method is memory-intensive and has a higher time complexity. In this paper, we propose a method of off-line signature recognition using Convolution Neural Network to achieve high accuracy multi-class classification with few trainings signature samples. Images are preprocessed using a series of image processing techniques to isolate the signature pixels from the background and noise pixels.

III. EXISTING SYSTEM

An artificial neural network, designed after the human brain, consists of interconnected nodes or neurons arranged in layers and is designed to adapt and learn from data. By recognition the data, identifying the pattern and predicting the future patterns of the inputs which are given to the ANN. The network breaks down input into layers of abstraction and learns through training examples, adjusting the strength of connections between nodes, or weights, until it can accurately perform the desired task based on a specified learning rule.

Support Vector Algorithm

Support vector machines (SVMs) are the machine learning algorithm that is supervised so that can be used for classification tasks and also to check the failure as of now they are mostly used for classification. They were initially introduced in the 1960s but they started developing them in the late 1990s. SVMs have a distinctive way of being implemented that differs from other machine learning algorithms.

They have gained popularity due to their ability to handle multiple continuous and categorical variables.

Working:

The fundamental idea behind an SVM model is to represent distinct classes in a hyperplane located in a multidimensional space. This hyperplane is generated iteratively by the SVM algorithm to minimize errors. The main objective of SVM is to divide the dataset into classes and identify a maximum marginal hyperplane(MMH).

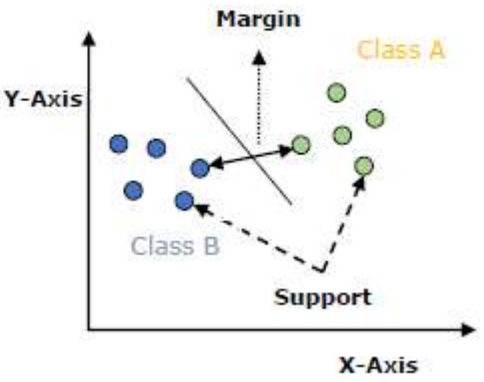


Fig 4. Support vector algorithm graph

The followings are important concepts in SVM

- **Support Vectors:** Data points that are closest to the hyper plane is called support vectors. Separating line will be defined with the help of these data points.
- **Hyper plane:** As we can see in the above diagram, it is a decision plane or space which is divided between a set of objects having different classes.
- **Margin:** It may be defined as the gap between two lines on the closet data points of different classes. It can be calculated as the perpendicular distance from the line to the support vectors. Large margin is considered as a good margin and small margin is considered as a bad margin.

The main goal of SVM is to divide the datasets into classes to find a maximum marginal hyper plane (MMH) and it can be done in the following two steps −

- First, SVM will generate hyper planes iteratively that segregates the classes in best way.
- Then, it will choose the hyper plane that separates the classes correctly.

Support vector machines (SVMs) are one of the supervised learning algorithms that can be applied to binary classification method or regression problems where many problems are encountered. SVMs are widely used in multiple areas like natural language processing, speech recognition, image recognition and computer vision etc. These algorithms aim to generate an optimal hyperplane, which serves as a decision boundary that maximizes the margin of separation between the two classes in the data. Support vectors are a part of the training observations used to support the optimal position of the decision surface. SVMs are a type of kernel method in machine learning and are sometimes referred to as kernel machines.

Training for a support vector machine has two phases:

1. The kernel trick is a technique used by support vector machines to transform input data (predictors) into a high-dimensional feature space. Instead of explicitly transforming the data, the kernel is specified to accomplish this task. As a result, it is unnecessary to compute the transformed feature space explicitly. This technique is referred to as the kernel trick.
2. Solve a quadratic optimization problem to fit an optimal hyper plane to classify the transformed features into two classes. The number of modified features is determined by the number of support vectors.

IV. PROPOSED METHOD

In this system, two phases are implemented namely, training and testing. In training phase, datasets of iris, faces and signatures are collected and preprocessed using image processing techniques. With the help of those datasets, convolutional neural network layers and training options, we can create a network like IRISNET, FACENET & SIGNNET for iris recognition, face recognition and signature recognition respectively. These nets are created using CNN technique.

Note: This process is completely involved with deep learning techniques.

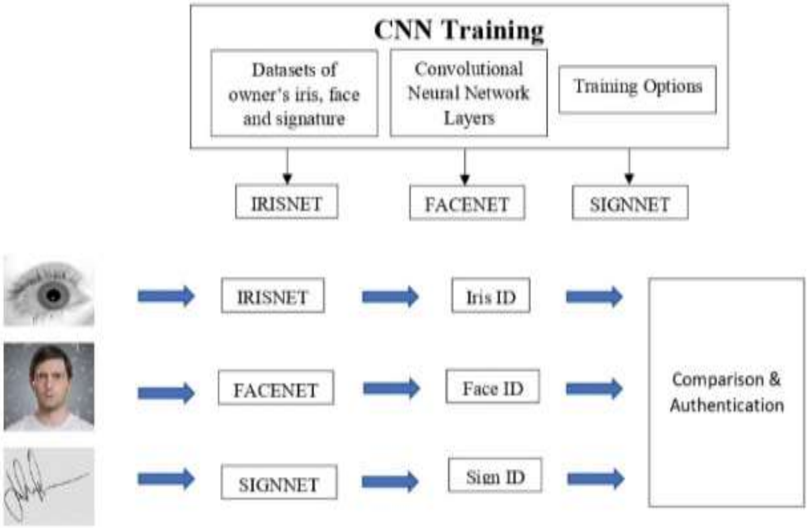

CNN Training
Datasets of owner's iris, face and signature
Convolutional Neural Network Layers
Training Options
IRISNET
FACENET
SIGNNET
IRISNET
Iris ID
FACENET
Face ID
SIGNNET
Sign ID
Comparison & Authentication

Fig 5. CNN Training Block Diagram

AI Training

The actual AI training phase includes three steps: training, validation, and testing. It is being trained by feeding data into the computer system to produce a specific prediction with each cycle. The parameters can be adjusted each time to make sure the predictions become more accurate with each training step.

It then verifies the algorithm by running validation data against the trained model. At this stage, new variables might need to be modified to improve the algorithm. When the validation stage has finished, the device can be checked using real-world data which do not have tags or labels. This is the time to see whether the algorithm is ready for its use.

To train a deep network from scratch, we need to gather a very large number of data set and design a network architecture that will learn the features and model. This is good for new applications, or applications that will have a large number of output categories. The method of training a neural network from beginning is not very common due to the large amount of data and long training times, to complete the training. Instead, most deep learning applications adopt the transfer learning approach, which involves fine-tuning a pretrained model. This approach entails using an existing network, such as Alexnet or GoogLeNet, and feeding it with new data containing classes that were not previously known.

By making adjustments to the network, it becomes feasible to carry out a fresh task, like classifying exclusively between dogs or cats instead of a thousand varied objects. This approach also offers the advantage of requiring less data (processing thousands of images, as opposed to millions), thus reducing computation time to mere minutes or hours. Another deep learning method is feature extraction, where a specific layer of the neural network responsible for learning a particular image feature is extracted and added to another machine learning model as an additional feature.

Training data is the part of the data from the dataset which we help our machine learning model to make predictions. This model will be run on this set of data exhaustively, churning out results which your data scientists can use to develop your algorithm. It’s the largest part of your overall dataset, comprising around 70-80% of your total data used in the project.

Validation data set contains input and target information, which the machine learning model has never encountered before. By testing the model on this data set, it can be determined whether it is capable of accurately identifying new examples. Validation also helps in detecting new values that can affect the model's performance. Overfitting is another issue that can be identified during validation, wherein the model is trained to identify specific examples that are too closely related to the training data. To address this, data scientists usually revisit the training data after validation and make adjustments to values and hyperparameters to improve the model's accuracy.

Testing data is introduced to check its real-world performance. Unlike validation data, testing data does not contain any tags or target information that can help the model. The model is required to make predictions based solely on the features of the testing data, which simulates the real-world scenario. This is the ultimate test for the model, where it is put to the test without any training wheels or supervision. Success on this test confirms whether all the efforts put into developing the model have been fruitful.

V. SIMULATION RESULT

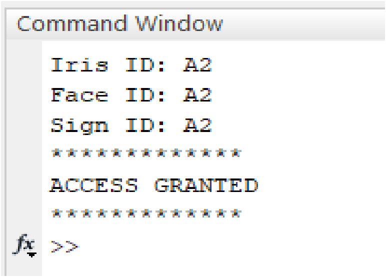
INPUT – 1

IRIS IMAGE 1

FACE IMAGE 1

SIGNATURE IMAGE 1

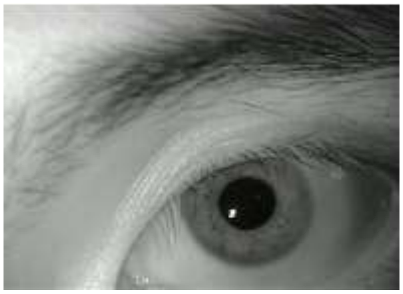
OUTPUT – 1



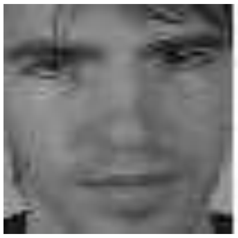
```
Iris ID: A2
Face ID: A2
Sign ID: A2
*************
ACCESS GRANTED
*************
>>
```

AUTHENTICATION RESULT

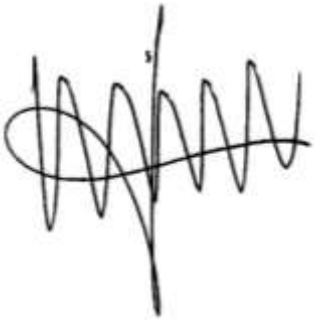
INPUT – 2



IRIS IMAGE 2

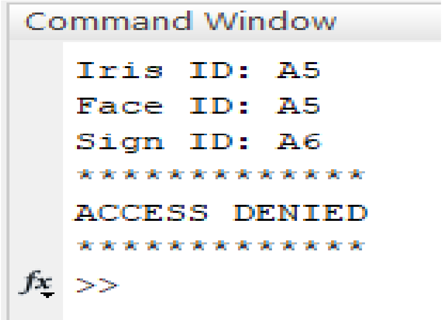


FACE IMAGE 2



SIGNATURE IMAGE 2

OUTPUT – 2



```
Iris ID: A5
Face ID: A5
Sign ID: A6
*************
ACCESS DENIED
*************
>>
```

AUTHENTICATION RESULT

VI. CONCLUSION

In this work, we have developed several recognition approaches like iris, face and signature and obtained several results. Firstly, we have trained IRISNET with iris dataset, FACENET with face dataset and SIGNNET with signature dataset, and then tested the networks with input iris, face and signature images. Our system produces the IDs of three images finally authentication is performed on the basis of IDs comparison. If all the IDs are same “Access Granted”, if not “Access Denied”

VII. REFERENCES

[1] C.S.S.Anupama, P.Rajesh, “Authentication using Iris”, International Journal of Innovations in Engineering and Technology (IJIET), Vol. 2 Issue 4 August 2013

[2] L. Li, X. Mu, S. Li and H. Peng, "A Review of Face Recognition Technology," in IEEE Access, vol. 8, pp. 139110-139120, 2020, doi: 10.1109/ACCESS.2020.3011028.

[3] K. Kancharla, V. Kamble and M. Kapoor, "Handwritten Signature Recognition: A Convolutional Neural Network Approach," 2018 International Conference on Advanced Computation and Telecommunication (ICACAT), 2018, pp. 1-5, doi: 10.1109/ICACAT.2018.8933575.

[4] Salman Khan; Hossein Rahmani; Syed Afaq Ali Shah; Mohammed Bennamoun; Gerard Medioni; Sven Dickinson, A Guide to Convolutional Neural Networks for Computer Vision, Morgan & Claypool, 2018.

[5] R. E. Twogood and F. G. Sommer, "Digital Image Processing," in IEEE Transactions on Nuclear Science, vol. 29, no. 3, pp. 1075-1086, June 1982, doi: 10.1109/TNS.1982.4336327.

[6] P. Sreekala., V. Jose, J. Joseph and S. Joseph, "The human iris structure and its application in security system of car," 2012 IEEE International Conference on Engineering Education: Innovative Practices and Future Trends (AICERA), 2012, pp. 1-5, doi: 10.1109/AICERA.2012.6306710.