IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

IRIS-BASED HUMAN IDENTITY RECOGNITION WITH DEEP LEARNING METHODS

Mr.V.Balu[#1], Rohith Santosh [#2], Sai Kiran [#3]

[#1]*Assistant professor, dept of cse, scsvmv university .*

[*2] *Student, dept of cse , scsvmv university .*

[#3] *Student, dept of cse , scsvmv university .*

Abstract - The computer system module in charge of user security is one of the most crucial ones.Simple logins and passwords have been shown to be vulnerable to hackers and unable to ensure high levels of efficiency.

The popular substitute is identity identification using biometrics. Iris as a biometric feature has drawn increased attention in recent years. It resulted from the exceptional efficiency and accuracy that this approach provided. The results of this interest can be seen in the literature.

Keywords - Iris-based human identity recognition, CNN, Transfer learning, Image segmentation, artificial neural networks.

I.INTRODUCTION

Such a challenge has an incredibly simple solution.Biometrics are the commonly known solution.Science is the field that recognises (or confirms) humans based on their quantifiable characteristics.

These characteristics can be categorised into three main categories: physiological (related to our bodies and appropriate measurements), behavioural (these are the traits we can learn, such as a signature), and hybrid, which combines physiological and behavioural characteristics.

We can infer that each computer system user (whose security system relies on biometrics) won't supply any additional passwords because he will be a real password by virtue of his measurably distinguishable characteristics.

Many studies and trials have demonstrated that the iris is one of the most crucial characteristics that may ensure excellent accuracy, effectiveness, and recognition rates. There are more than 250

different components in this feature. They are all employed to characterise human identity (in the form of feature vector). It has also been established in the literature that these feature vectors are entirely distinct for a single person's left and right eyes, and that this is true even in the case of identical twins. They each have unique irises (feature vectors are completely different). The fact that iris is extremely challenging to fake is crucial. It must be acknowledged, though, that in these works, only straightforward iris-based biometrics systems were employed. It implies that such solutions do not take into account iris livens and are therefore susceptible to print attack (with iris photo).

But, iris has one very significant drawback: it is very difficult to obtain high-quality iris samples without specialist equipment. In some circumstances, assistance from a skilled ophthalmologist is required to finish the task. Of course, modern smartphones with excellent cameras, like the Apple iPhone 12 Max or Samsung Galaxy S20+, can also be used to capture iris samples.

But once more, a second person's assistance is required. We can utilise specialised sensors that are sold on the market to gather these photos on our own. But, they are very expensive, and some of them even require certain lighting conditions to produce accurate, high-quality photographs. A sizable portion of this effort also has to do with the testing procedures employed in the quality assurance process. To boost algorithm precision, the authors employed Agile methodology to develop the solution initially in a step-by-step fashion. We evaluated the quality of the generated solutions at each level. It functioned as the primary metric by which we assessed whether progress had been made.

The prevention of spoofing must be taken into account when designing iris-based security solutions. Positive recognition based on printed images rather than actual samples is the most frequently found vulnerability in biometrics systems. It is specifically linked to iris-based systems. This issue was thoroughly discussed in. The authors of the paper made the case that print attack photos of a live iris, the use of contact lenses, and the combination of both can significantly affect the system's ability to identify false positives. The IIIT-WVU iris dataset was used for all trials. Also, the authors revealed a cutting-edge method for stopping such assaults using a deep convolutional neural network.

II.LITERATURE REVIEW

[1] Gupta P, Behera S, and Vatsa M, Singh R: In this study, iris recognition with spoofing assaults is reviewed, and their impact on recognition performance is examined. The spoofing approach specifically uses print attack with contact lens variants. It has been found that contact lenses and print attacks, both separately and together, can drastically alter intra- and inter-personal distributions, increasing the likelihood that iris recognition systems would be fooled.

[2] Rana HK, Azam MS, Akhtar MR, Qunin JMW, Moni MA: This paper suggests a method for using Principal Component Analysis (PCA) based on Discrete Wavelet Transformation (DWT) to extract the best features of an iris and shorten the processing time required for classifying iris templates. Reducing the resolution of the iris

template is the purpose of employing DWT in conjunction with PCA.

[3] Arora S, Bhatia MPS: Studies done on the IIIT-WVU iris dataset reveal that contact lenses, print attack photos of live iris images, and a combination of both can be quite effective at fooling iris recognition systems. In contrast to current state-of-the-art methodologies, the article uses deep convolutional neural networks to detect such spoofing tactics with better results.

[4] Iris recognition has been a hotly debated topic in recent years because to the vast range of security applications it has, from border control at airports to homeland security. In the past, several features and methods have been suggested for iris recognition. In this paper, they suggest a residual convolutional neural network (CNN)-based end-to-end deep learning architecture for iris identification that can simultaneously learn the feature representation and carry out recognition.

[5] Minaee S, Abdolrashidi A : In several field and laboratory studies, the author's algorithms for iris pattern recognition have produced no false matches in more than a million comparison tests. The recognition principle is established on the basis that a statistical independence test on the iris phase structure collected by multi-scale quadrature wavelets failed. With 249 degrees of freedom and 3.2 b/mm/sup 2/ of discrimination entropy over the iris, the combinatorial complexity of this phase information across various people enables very accurate real-time determinations about personal identity.

III.PROPOSED SYSTEM

In our intended technique, we execute the classification of either the Convolution Neural Network (CNN) based transfer learning (MobileNet) or deep learning method for Iris-based Human Identity Identification identification. Several techniques for iris-based human identification recognition that are based on image analysis. So, accurate classification is crucial for the right nutrition that would be made possible by applying the strategy we have suggested. where the CNN method is being used to classify the photos. The segmentation of the iris portion occurs following categorization. This is a block schematic of the suggested method.

Block Diagram:

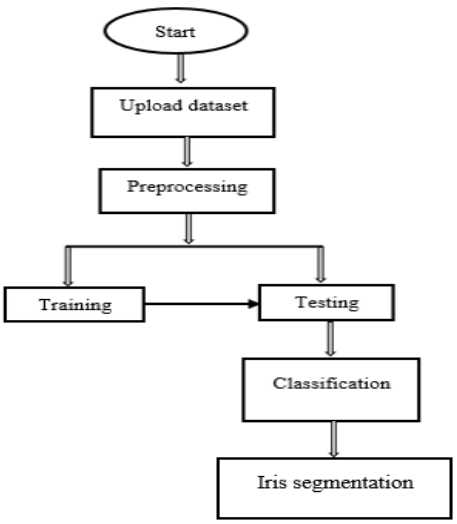

Fig 1. Block diagram of proposed method

Advantages:

- Accurate classification
- Less complexity
- High performance

IV.ARCHITECTURE

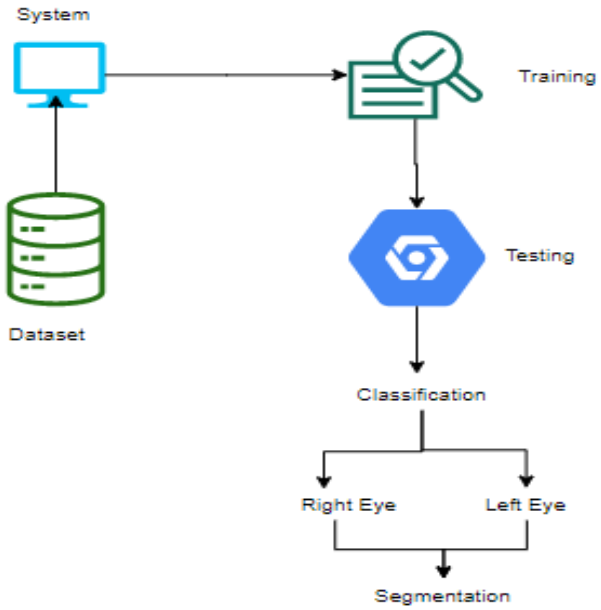

Fig 2.System Architecture

V.OUTPUT

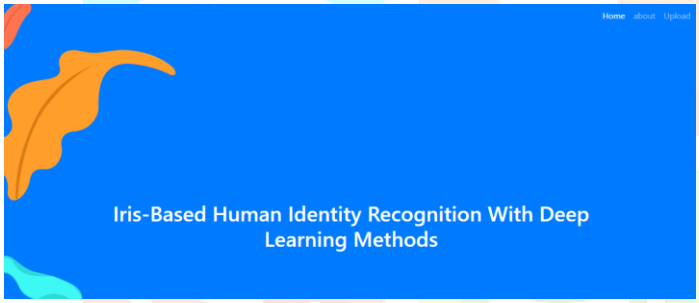

Fig 3.Home Screen

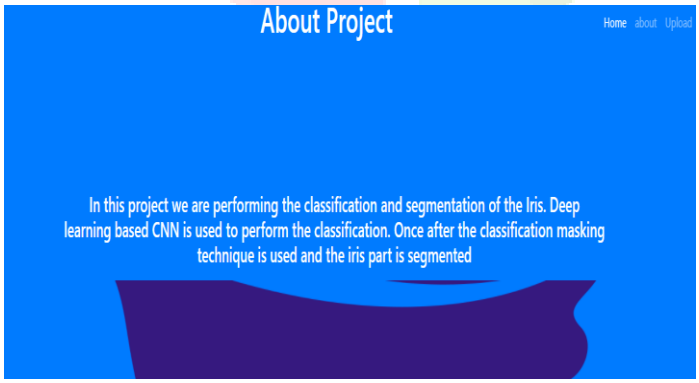

Fig4.About Project

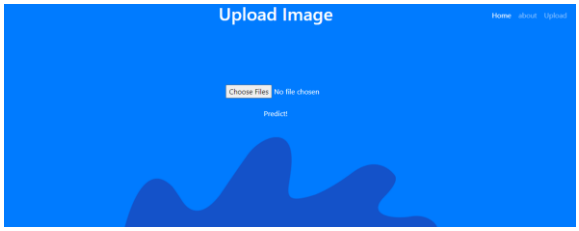

Fig 5. Image Uploading page

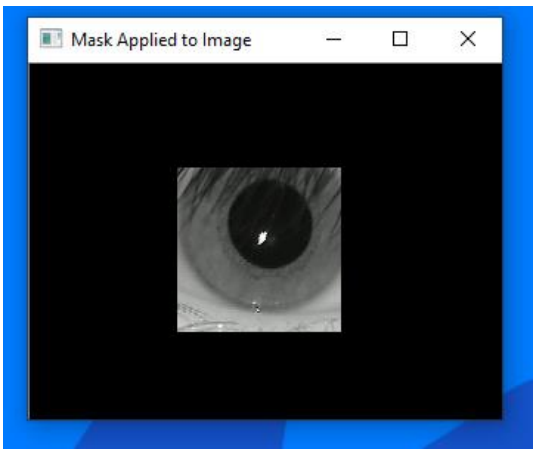

Fig4: Model choosing

VI.CONCLUSION

With the use of deep learning, we were able to properly classify the left or right eye image in this research. Here, we have used CNN training to take into account the dataset of eye classes. Following training, the user can input a picture and verify the results for classification. The iris portion of the categorised output is segmented following classification.

VII.FUTURE SCOPE

In the future, this procedure might be expanded to include biometrics. With this kind of work, biometrics relying mostly on the iris portion will be more advantageous.

REFERENCES

[1] Gupta P, Behera S, Vatsa M, Singh R (2014) On iris spoofing using print attack, In IEEE on 22nd international conference on pattern recognition on August 2014.

[2] Rana HK, Azam MS, Akhtar MR, Qunin JMW, Moni MA (2019) on "fast iris recognition system through optimum feature extraction". PeerJ Comput Sci

[3] Arora S, Bhatia MPS (2020) Presentation attack detection for iris recognition using deep learning. Int J Syst Assur Eng Manag.

[4] Minaee S, Abdolrashidi A (2019)on " iris recognition using a deep learning approach" on IEEE.

[5] Daugman J (2004) How iris recognition works. IEEE Trans Circuits Syst Video Technol 14(1):21–30