International Journal of Innovative Research in Engineering
Volume 5, Issue 1(January-February 2024), PP: 29-31.
https://www.doi.org/10.59256/ijire.20240501006
www.theijire.com
ISSN No: 2582-8746

Multimodal Biometric Login System Using Face and Signature

Vanithamani.K[1], Vishnu Prasanna.T.S[2], Srinivaas.R[3], Srinivasan.P.K[4], Vimal.K.S[5]

[1]Assistant Professor, Department of Computer Science and Engineering, K.L.N. College of Engineering and Technology, Sivagangai, Tamilnadu, India.
[2,3,4,5] Students, Department of Computer Science and Engineering, K.L.N. College of Engineering and Technology, Sivagangai, Tamilnadu, India.

How to cite this paper:
Vanithamani.K[1], Vishnuprasanna.T.S[2], Srinivaas.R[3], Srinivasan.P.K[4], Vimal.K.S[5], "Multimodal Biometric Login System Using Face and Signature", IJIRE-V5I01-29-31.

Copyright © 2023 by author(s) and 5th Dimension Research Publication.
This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).
http://creativecommons.org/licenses/by/4.0/

Abstract: *Biometrics has developed to be one of the most relevant technologies used in Information Technology (IT) security. Uni-modal biometric systems have a variety of problems which decreases the performance and accuracy of these systems. One way to overcome the limitations of the Unimodal biometric systems is through fusion to form a multimodal biometric system. Hence this process is developed based on Multimodal Biometric system based on Face, Finger print, Signature etc. Multimodal biometric system employing Convolutional Neural Networks (CNNs) for effective feature extraction and classification. The system combines facial and signature biometrics, harnessing the unique advantages of each modality to create a more resilient and accurate authentication framework. Multimodal biometric system with CNN integration holds promise for applications in secure access control, financial transactions, and other domains where reliable authentication is crucial. Its adaptability and scalability make it a viable solution for addressing the evolving challenges in biometric security systems.*

Key Word: *Unimodal biometric system , Multimodal Biometric system , Convolutional Neural Networks (CNNs),deep learning.*

I.INTRODUCTION

Face and signature identification are common biometric techniques used for authentication and identity verification. They can be used individually or in combination to enhance security in various applications. Here's an overview of both methods. Face identification, often referred to as face recognition, is the process of identifying an individual based on their facial features. It is a widely used biometric method for identity verification and access control. Signature identification, also known as signature verification or handwriting recognition, is the process of authenticating an individual based on their handwritten signature. Both face and signature identification has their advantages and limitations. While face identification is non-intrusive and widely used, it may have privacy concerns. Signature identification, on the other hand, is commonly used for document verification and legal purposes but can be more vulnerable to forgery. Depending on the specific usecase, one or both of the methods may be employed for identity verification.

II.RESEARCH AND FINDINGS

Today handwritten signatures popularly used and acceptable means of biometric authentication. There are two cases of signature verification: Online and offline verification systems. Usually online more useful than offline, because of the availability of information like stroke order, writing speed, pressure, etc. But these performances need the cost for special hardware for recording the pen-tip path, improving its system cost and decreasing the actual application situations. In the offline system, just a static image of the signature is available, it is more complicated than an online system because dynamic information is not available and it is hard to reach them from the offline images. Offline signature verification depends on pattern recognition; signatures are described using fixed-size feature vectors. There are multiple ways for signature verification; one of them is by using graphs and structural pattern recognition.

Biometric methods that rely on the evidence associated with a one particular well spring of information for validation are actually labeled as Unimodal method. Unimodal biometric methods endure an assortment of problems, for instance, Commotion within detecting information, Intra class variations and Uniqueness capability. The confinements of unimodal biometric structure lead to substantial False Acceptance Rate (FAR) along with False Rejection Rate(FRR),limited splitting up skill, top bound within delivery therefore the multimodal biometric product is designed to satisfy the strict delivery demands. A biometric os and that is determined by the nearness of several pieces of evidence of specific identification is known as multimodal biometric structure

In our daily lives, we often remember and recognize people by looking at their faces. This is a part of the body that is highly visible and is important for interaction. We store information of a face and later use that information for recognition and matching purposes. This mechanism can be used by machines to recognize and authenticate a human being with the increasing importance of technology in business and human lives where security has become a critical concern for modern applications.

Users' authentication is the most important part of securing an application from unauthorized access. For this, knowledge-based, token-based and biometric based systems can be used. Traditional knowledge-based and token-based systems are losing appeal due to the issues associated with their usage. This situation has increased the importance of biometric (what we are) characteristics rather than knowledge (what we know) and token (what we have) approaches. In our country there many types of login systems are used such as login by punch card, user id or password. But in these systems, there is possibility of misusing the systems through mutual understanding. The developed smart system can overcome the previously developed systems' limitations. The system checks individual user's face with existing stored faces, that's why there is no chance of misuse.

III.SYSTEM IMPLEMENTATION

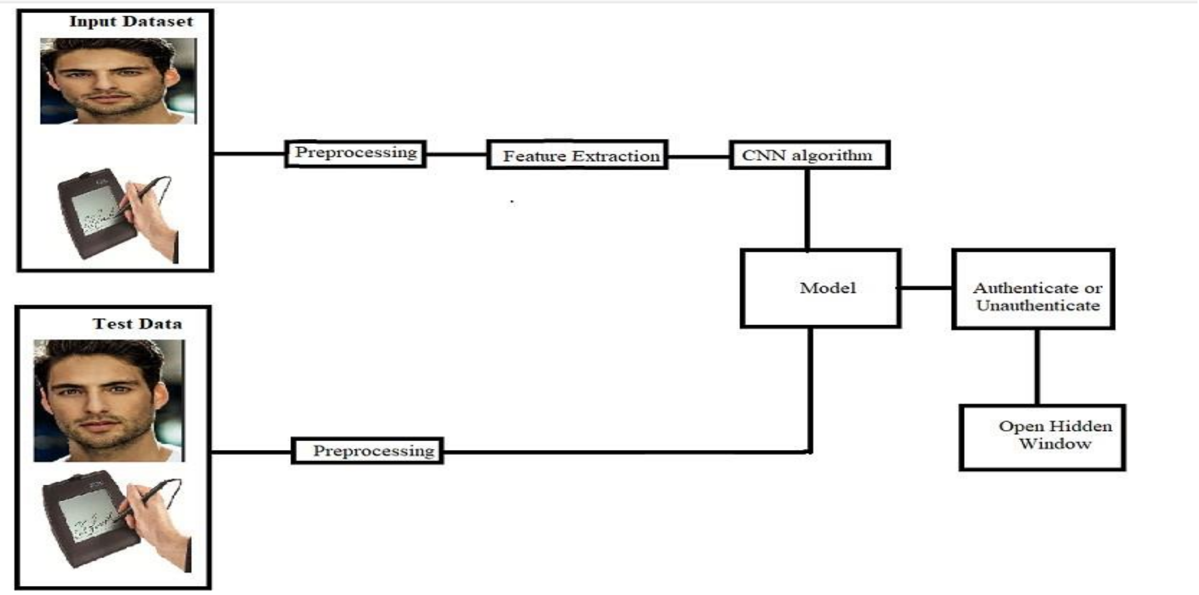

Figure: Flow Chart

These diagrams help us understand the flow of our proposed system in a simple way. The input is consisting of training and testing data along with a Facial image and Signature, is utilized in authentication process.

1. Preprocessing
Image Resize

- In computer graphics, image scaling is the process of resizing a digital image. Scaling is a non-trivial process that involves a trade-off between efficiency, smoothness and sharpness. With bitmap graphics, as the size of an image is reduced or enlarged ,the pixels that form the image become increasingly visible, making the image appear "soft" if pixels are averaged, or jagged if not.
- With vector graphics the trade-off may be in processing power for re-rendering the image, which may be noticeable as slow re-rendering with still graphics, or slower frame rate and frame skipping in computer animation.

2. Feature Extraction

A CNN is not only a deep neural network with many hidden layers but also a large network that simulates and understands stimuli as the visual cortex of the brain processes .CNN's output layer typically uses the neural network for multiclass classification. CNN uses the feature extractor in the training process instead of manually implementing it. CNN's feature extractor consists of special types of neural networks that decide the weights through the training process. CNN provides better image recognition when its neural network feature extraction becomes deeper (contains more layers), at the cost of the learning method complexities that had made CNN in efficient and neglected for some time. CNN is a neural network that extracts input image features and another neural network classifies the image features. The input image is used by the feature extraction network. The extracted feature signals are utilized by the neural network for classification. The neural network classification then works on the basis of the image features and produces the output. The neural network for feature extraction includes convolution layer piles and sets of pooling layers. As its name implies, the convolution layer transforms the image using the process of the convolution. It can be described as a series of digital filters. The layer of pooling transforms the neighboring pixels into a single pixel. The pooling layer then decreases the image dimension.

3. Feature Matching Process

Feature matching means finding corresponding features from two similar datasets based on a search distance. One of the datasets is named source and the other target, especially when the feature matching is used to derive rubber sheet links or to transfer attributes from source to target data. These datasets overlap each other but are not perfectly aligned due to inconsistent data collection, changes over time, or other reasons. The feature matching process analyzes the source and target topology, detects certain feature patterns, matches the patterns, and matches features within the patterns. The accuracy of feature matching depends on data similarity, complexity, and quality. In general, the more similar the two datasets, the better matching results. Normally, a high percentage of successful matching can be achieved, while uncertainty and errors may occur and require post inspection and corrections. Feature attributes can optionally help determine the right match in feature matching. If one or more pairs of match fields are specified ,spatially matched features are checked against the match fields. For example, if one source feature spatially matches two candidate target features ,but one of the target features has matching attribute values and the other doesn't, then the former is chosen as the final match. The condition of attribute match affects the level of confidence of the feature matching. Image classification using Convolutional Neural Networks(CNNs)is a powerful application of deep learning in computer vision. CNNs are designed to automatically learn and extract hierarchical features from images, making them particularly effective for recognizing patterns and objects. In this process ,the input image is fed through a series of convolutional layers, which apply filters to detect features like edges, textures, and shapes. Activation functions introduce non-linearity, and pooling layers down sample the spatial dimensions, reducing computational complexity. The learned features are then flattened and passed through fully connected layers, acting as classifiers to make predictions. The final layer often utilizes a soft max activation function to output probabilities for different classes. During training, the network's parameters are optimized using back propagation and an appropriate loss function. This enables the CNN to learn and generalize patterns from a labeled dataset. With successful training, the CNN can accurately classify new, unseen images into predefined categories, demonstrating its efficacy in various real-world applications, such as object recognition, medical image analysis, and autonomous vehicles.

4. Performance Analysis

The performance of the process is measured in terms of performance metrics like Accuracy ,Sensitivity, Specificity and time consumption.

- TP - is the total number of correctly classified foreground (true positives).
- TN - is the total number of wrongly classified foreground (true negatives).
- FN - is the total number of false negatives, which accounts for the incorrect number of foreground pixels classified as background(false negatives).
- FP - is the total number of false positives, which means the pixels are incorrectly classified as foreground(false positives).The performance values were calculated for each frames of the input video based on the metrics described above.

IV.CONCLUSION

In conclusion, the integration of multi-modal biometrics, particularly combining face and signature authentication through deep learning ,represents a pivotal step forward in the quest for robust and reliable identity verification systems. Deep learning's ability to extract complex and high-level features from diverse biometric data sources enhances the accuracy and security of the authentication process. By leveraging neural networks like Convolutional Neural Networks (CNNs) these systems effectively capture and analyze the unique characteristics of both facial and hand written signatures. This fusion of information not only significantly enhances identification accuracy but also mitigates the potential vulnerabilities of single-modal systems, such as susceptibility to spoofing or false rejections.

References

1. *A.AlAbdulwahid, N.Clarke, I.Stengel ,S.Furnell, and C.Reich, ‘‘Continuous and transparent multimodal authentication: Reviewing the state of th eart,’’ Cluster Comput.,vol.19,no.1,pp.455–474,Mar.2016.*
2. *P. Arias-Cabarcos, C. Krupitzer, and C. Becker, ‘‘A survey on adaptive authentication,’’ACMComput.Surv.,vol.52,no.4,pp.1–30,Sep. 2019.*
3. *S. Ayeswarya and J.Norman,‘‘A survey ond ifferent continuous authentication systems,’’Int.J.Biometrics,vol.11,no.1,p.67,2019.*
4. *C.Lisetti and C.LeRouge,“Affective computing intele-home health:Design science possibilities in recognition of adoption and diffusion issues,”inProc.37thIEEEHawaii Int.Conf.Syst.Sci.,Hawaii,USA,Jan.2004,pp.348–363.*
5. *Y. Pang, Y. Yuan, and X. Li, “Iterative subspace analysis based on feature line distance,” IEEE Trans. Image Process. , vol. 18, no. 4, pp. 903–907, Apr.2009.*
6. *P. J. Phillips, J. R. Beveridge, B. A. Draper, G. Givens, A. J. O’Toole, D. S.Bolme, J. Dunlop, Y. M. Lui, H. Sahibzada, and S. Weimer, “An introduction to the good, the bad, &the ugly face recognition challenge problem,” in 2011IEEE International Conference on Automatic Face & Gesture Recognition and Workshops (FG). IEEE,2011,pp.346–353.*
7. *R. Ptucha and A. Savakis, “LGE-KSVD: Flexible Dictionary Learning for Optimized Sparse Representation Classification,” in 2013 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW). IEEE, 2013,pp.854–861.*
8. *M. H. Siddiqi, A. M. Khan, T. C. Chung, and S. Lee, “A precise recognitionmodelforhumanfacialexpressionrecognitionsystem,”inProc.26thIEEECan.Conf.Elect.Comput.Eng.,2013.*
9. *M. Singh, R. Singh, and A. Ross, ‘‘A comprehensive overview of biometric fusion,’’Inf.Fusion,vol.52,pp.187–205,Dec.2019.*
10. *Y.Taigman, M.Yang, M.Ranzato, and L.Wolf, “Deepface: Closing the gap to human-level performance in face verification,” in 2014 IEEE Conference on Computer Vision and Pattern Recognition(CVPR).IEEE,2014,pp.1701–1708.*