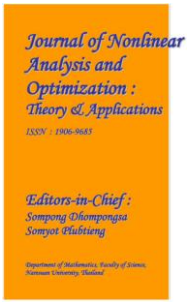
Journal of **N**onlinear **A**nalysis and **O**ptimization
Vol. 15, Issue. 1, No.7 : 2024
ISSN : **1906-9685**



BIOMETRIC AUTHENTICATION METHOD AS FACE REGONIZATION IN WEB BASED SYSTEM

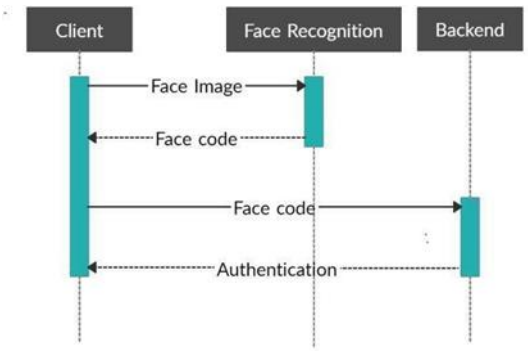
Mr. T Ravin Prakash Student, BScDCFS Department of Digital Cyber Forensic Science Rathiam College of Arts and Science, Coimbatore-21
Ms. V. Yogashri Assistant Professor Department of Digital Cyber Forensic Science Rathiam College of Arts and Science, Coimbatore-21

Abstract:
Online information systems currently heavily rely on the username and password traditional method for protecting information and controlling access. With the advancement in biometric technology and popularity of fields like AI and Machine Learning, biometric security is becoming increasingly popular because of the usability advantage. This paper reports how machine learning based face recognition can be integrated into a web-based system as a method of authentication to reap the benefits of improved usability. This paper includes a comparison of combinations of detection and classification algorithms with Face Net for face recognition. The results show that a combination of MTCNN for detection, Face net for generating embeddings, and Linear SVC for classification out performs other combinations with a 95% accuracy. The resulting classifier is integrated into the web-based system and used for authenticating users.

Keywords –
Face Net, MTCNN, Face Recognition, Machine Learning, Biometric Authentication, Linear SVC

Introduction:

Information and Communication Technology us-age has witnessed rapid growth in the past decade all around the world. A bigger percentage of the population has laptops, personal computers, and smartphones making it easy to access the internet and thus changing the lives of millions of people. All web-based systems that have users and store personal information about the users require a mechanism to keep track of their users' information. Most commonly every user of the system is assigned an instance in the database that represents them (their identity). To protect the user identity, an authentication and authorization mechanism is implemented to control access to certain information. The most common method in web-based systems is authentication using passwords. This leads to promotion of biometric-based authentication. The primary motivation of biometric authentication is usability users are not required to remember the passwords, there is nothing for them to carry, biometric systems are generally easy to use, and scalable in terms of the burden exerted onto the users.



Biometric authentication is the automatic authentication that identifies a person by

analyzing their physiological and/ or behavior features. In the past two decades, both physiological and behavior characteristics have been used in biometric authentication systems. Physiological features are attributed to the person's body shape such as the face, palm prints, DNA, etc. Behavioral characteristics are attributed to the person's behavior: typing speed, voice, and articulation.

Previous Generations:

Biometric has ancient roots, with fingerprints and palm prints used historically for identification. Modern technology has expanded the possibilities for biometric systems, ensuring robust security. Biometric traits are highly individual and tough to replicate, enhancing protection against fraud and identity theft. While convenient, concerns include privacy issues and potential inaccuracies. Despite these concerns, biometric authentication is rapidly gaining popularity in various applications, from smartphone access to healthcare security. This article delves into the history, techniques, applications, and challenges of biometric authentication.

Working model:

Our Approach on face recognition consists of three stages, that is given an image, we perform face localization, face embeddings generation using Google's Face Net pretrained model, and classification using the Linear SVC classifier.

- Data Collection: In a case study on 100 different people, a total of 1424 images from the volunteers. Captured using a 12MP dual-lens camera of the technocam on12 air smart phone, the images appeared in different orientations and lightings. The number 1424 is that which was obtained after performing data cleaning.
- Hardware Setup: The training was done on a personal computer. AHP Pro Book450G3, with 8192 MBRAM, Intel(R) Core(TM) i5-6200UCPU@2.30GHz(4CPUs)2.4 GHz processor, and AMDRadeon (TM)R7 M340 graphics card with 2GB dedicated VRAM.
- Face Detection: For the case of face detection, two of the most commonly used ways of face detection were com-pared; The Viola-Jones Haarcascade classifier: It is based on the Viola-Jones Object Detection frame-work. This frame work has a quiet high (true positive rate) detection rate and a very low false positive rate making the algorithm a robust one that also processes the images quickly. The main objective is face detection not recognition: it distinguishes faces from non-faces which is the first (preprocessing) step recognition. The framework follows four main steps:HaarFeatureSelection,CreatinganIntegralImage,Ad boostTrainingandtheCascadingClassifiers.

Key enabling technologies:

Face Recognition:A FaceNet model pre-trained on a VGGFace2 dataset consisting of 3.3M faces and 9000classes in an inception ResNet v1 architecturewas used. The pretrained model expects160×160 RGB images. The model was converted into a keras compatible version. Theconvertedmodelwasusedtogenerateembeddingsforallimagesinthefacesdataset.Foreachfaceimagein thefacesdataset,anarrayof512differentweightsuniquelyrepresentingthefacewasgenerated.Anewdataset offaceembeddingswaspreparedandcompiledforclassificationpurposes. The generated embeddings are used to create a new dataset consisting of face embeddings. Table I below shows information aboutthepretrained Facenet model.

Classification: Linear SVC: The classificationmodelherewastrainedwitharegularparameter,randomstate = 0, and tuned with a hyperparameter C = 1. It took approximately 14 seconds totrainthis model, theaveragevalidationaccuracywas 0.93.

- RandomForest:Theclassificationmodelwascreatedwitharegularparameter,random state = 0, and tuned with a hyperparameter n estimators = 1000. The training for thismodeltook approximately120seconds.

Theaveragevalidationaccuracywas91%.Eachoftheclassificationalgorithmswasevaluatedwithmetrics:pr ecision,recall,accuracy,andthe confusion matrixto visualizewrongclassifications.

Potential Applications:

- Accuracy: The accuracy of face recognition technology has significantly improved overthe years,

with state-of-the-art models achieving close to human-level performance. However,there is still a possibility of false positives and false negatives, which can result in Accuracy.

• Security:Facerecognitiontechnologycanofferahighlevelofsecuritysinceitisdifficultto forge or manipulate facial features. However, there is a risk of biometric data theft, whichcould compromise the security of the system. Thus, it is essential to implement strict securityprotocolsto protect theuser's biometric data.

• User Experience: Face recognition technology provides a convenient and user-friendlyauthentication method, as users do not need to remember and input passwords or tokens.However, some users may not feel comfortable sharing their facial information or may haveprivacyconcerns,soitisimportanttoprovidethemwiththeoptiontouseotherauthenticationmethods.

• Integration: It is necessary to ensure that the face recognition technology is integratedproperly with the web-based system and its components, such as the database, applicationserver, and user interface.

Challenges:

- Privacy Concerns: Biometric authentication systems store sensitive information about individuals, such as their fingerprints or facial features. If this information falls into the wrong hands, it can be used for identity theft or other malicious purposes.
- False Positives: Biometric authentication systems may sometimes incorrectly identify individuals, leading to false positives. For example, a fingerprint scanner may not recognize a person's fingerprint if it's dirty or smudged. This can lead to frustration and inconvenience for users.
- High cost: Biometric authentication systems can be expensive to implement and maintain. The hardware and software required for biometric authentication can be costly, and the systems need to be regularly updated and maintained to ensure their effectiveness

Conclusion:

In conclusion, face recognition technology has emerged as a popular method of authentication in web-based systems due to its ease of use, speed, and accuracy. It offers several advantages over traditional authentication methods, such as passwords or PINs, which can be easily forgotten, stolen, or hacked. By using face recognition technology, web-based systems can provide a more secure and seamless user experience while protecting sensitive data and preventing unauthorized access. Additionally, face recognition can also be used for multi-factorauthentication, which provides an additional layer of security and helps to preventidentitytheft and fraud.However, there are also concerns regarding the use of face recognition technology,particularly regarding privacy, surveillance, and potential biases. It is important forweb-based systems to implement appropriate safeguards, such as data encryption, secure storage, and transparent policies, to protect user privacy and prevent misuse of the technology.

References:

1. *van Oorschot, P. C. (2020). User Authentication-Passwords, Biometrics and Alternatives. https://doi.org/10.1007/978-3-030-33649-3 3*

2. Hargrave, M. (2020). Deep Learning. https://www.investopedia.com/terms/d/deep-learning.asp#:

3. *D. Sandberg, "Facenet." 2018. https://github.com/davidsandberg/facenet.*

4. SAS. (2020). Machine Learning. https://www.sas.com/en us/insights/analytics/machinelearning.html

5. Luxand. (n.d.). Face recognition widget for your website. https://luxand.cloud/widget

6. T. Nyein and A. N. Oo(2019) , "University Classroom Attendance System Using FaceNet and Support Vector Machine,"

7. O. M. Parkhi, A. Vedaldi, and A. Zisserman,(2015) "Deep FaceRecognition,"

8. B. Prihasto et al., "A survey of deep face recognition in thewild," 2016

9. H. Tania, "keras-facenet," 2018.

10. "Geogia Tech Face Database."http://www.anefian.com/research/face rec o.htm.