

IDENTITY VERIFICATION WITH DIGITAL DOCUMENTS USING LIVE IMAGE

D.DURGADEVI, N.MONALI, G.DHARANISHREE, Mr. R.BABU

Student, Information Technology, Rajalakshmi Engineering College, Tamil Nadu, India

Student, Information Technology, Rajalakshmi Engineering College, Tamil Nadu, India

Student, Information Technology, Rajalakshmi Engineering College, Tamil Nadu, India

Assistant Professor, Information Technology, Rajalakshmi Engineering College, Tamil Nadu, India

ABSTRACT

Verification is important in our daily life by showing our ID documents containing face images, such as passports and driver licenses, to human operators. Because of labor intensiveness and unreliableness this process is slow. So that high accuracy is needed for matching ID document photos to live face images in real time. Here, we use face recognition in digital documents an automation system to meet this objective. To overcome this shortcoming, a method called dynamic weight imprinting (DWI) is used which recognizes the trained data of the human.

Keyword : - Automation System, Dynamic Weight Imprinting(DWI).

1. INTRODUCTION

Information technology has developed rapidly in recent years, data protection is more necessary than ever. Numerous activities in our daily life require us to verify who we are by showing our ID documents containing face images, such as passports and driver licenses, to human operators. However, this process is slow, labor intensive and unreliable. As such, an automated system for matching ID document photos to live face images in real time and with high accuracy is required. We first show that gradient-based optimization methods converge slowly (due to the underfitting of classifier weights) when many classes have very few samples, a characteristic of existing ID-selfie datasets. To overcome this shortcoming, to update the classifier weights, which allows faster convergence and more generalizable representations. Next, a pair of sibling networks with partially shared parameters are trained to learn a unified face representation with domain-specific parameters. Cross-validation on an ID selfie dataset shows that while a publicly available general face matcher.

1.1 EXISTING SYSTEM

In the existing system human operators are used to verify our identity using passports, driving licences which contain our face images. However, this process is slow, labor intensive and unreliable. As such, an automated system for matching ID document photos to live face images in real time and with high accuracy is needed. After verifying a traveler's identity by face comparison, the traveler is allowed to enter. For ID matching they are comparing scanned documents or digital documents. For example, access control, physical security and international border crossing require us to verify our access (security) level and our identities. To verify who we are by showing our ID documents containing face images. such as passports, PAN card, Voter id, driver licenses to human operators.

1.2 PROPOSED SYSTEM

The new automation system deals with identity verification with digital documents using live image for matching ID document photos. Data is stored in different nodes, and anyone who wishes to modify a particular internal datum must request that other nodes modify it simultaneously. Thus, the system is highly reliable. We developed a decentralized application and designed a certificate system in which the data gets trained by using a KNN algorithm.

The data is incorruptible, encrypted, and trackable and permits data synchronization. The user will get verified by a live face capture instead of a scanned or digital document photo and compare the user live face with verified document face. For example, while crossing international borders require us to verify our access (security) level and our identities. A practical and common approach to this problem involves comparing an individual's live face to the face image found in his/her ID document. A QR code is generated as a result of uploading necessary documents in the server.

2. ARCHITECTURE DIAGRAM

This model has been proposed for identity verification with digital documents using live image. In the figure.1 shows, Initially, the user registers into the application and a request is sent to the server for authentication. Only if the server approves the request the user can login into the account, and a UID will be generated and sent to the registered mail id so that the user can use that to login into his account. After login the certificates such as Pan card, Aadhar card ,voter id, SSLC certificate are uploaded. The server will review the certificates and accept or decline the certificates. If a user wants to apply for a passport or an entry pass for border crossing ,there is a need for certificates so he sends a request to the server, then the QR will be generated which contains the trained face image of digital documents. Then the user will forward the QR code to the verifying authority. Then the verifying authority compares the live face image with the trained face image and if the details are correct then the pass will be issued.

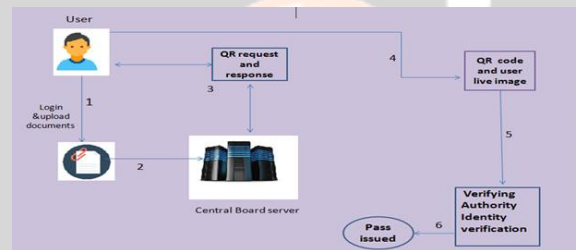


Fig -1: Architecture Diagram

2.1 USER REGISTRATION AND AUTHENTICATION

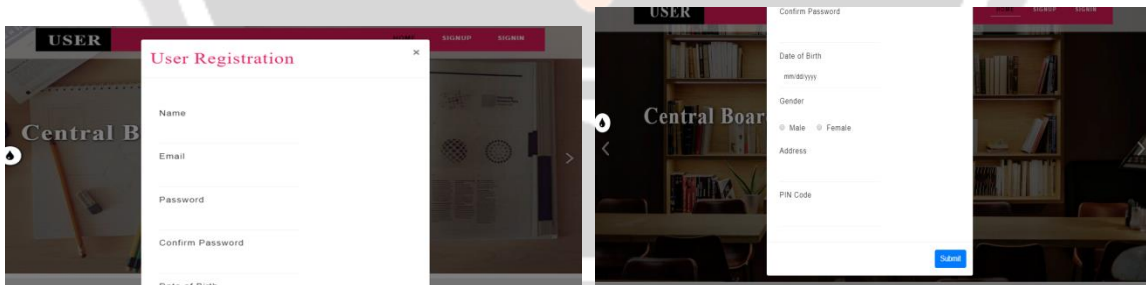


Fig -2: User Registration

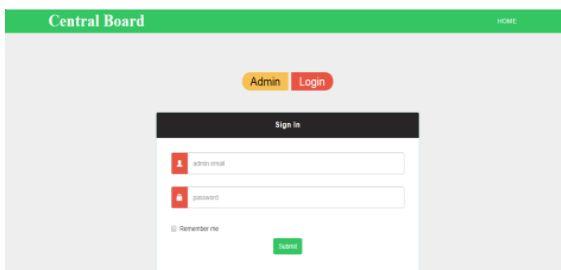


Fig -3: Central Board Server Login

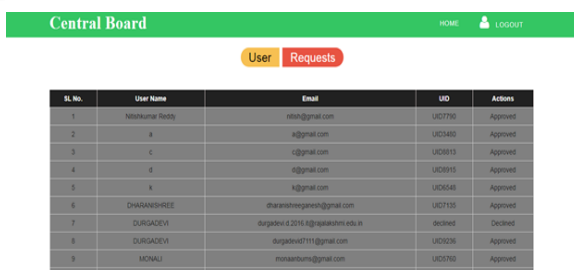


Fig -4:Accept/Decline User Request

2.2 USER UPLOAD CERTIFICATE AND FACE VERIFICATION

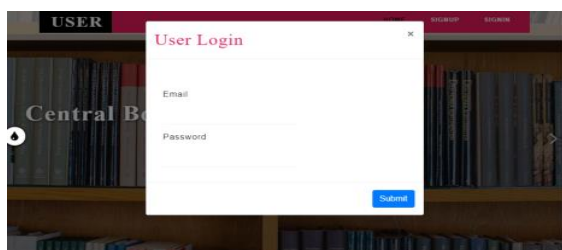


Fig -5:User Login

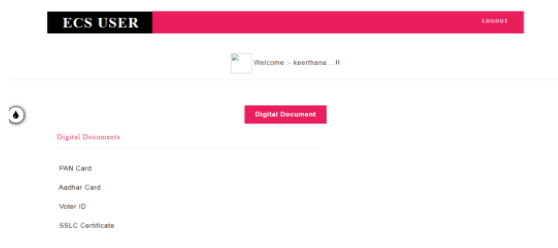


Fig -6:User Upload Certificate

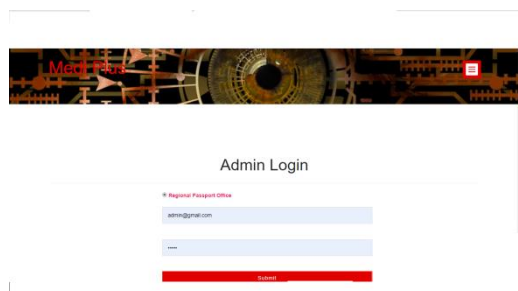


Fig -7:Verification Authority Login



Fig -8: Live Face Comparison

3. MODULE EXPLANATION

The user needs to register the details in the central board server by login and upload the certificates, The image in the document will get trained and stored in the block chain, and whenever the user needs the certificates they can get the certificates by requesting the central board server. As a result QR code is generated by the ECS which contains the encrypted data of digital documents and provided to the user via the Central Board server. Then the user forwards the QR code to verification authority and the encrypted QR code will be decrypted by the QR scanner then the trained digital document image will be compared with the user's live face . If both will be matched, a digital document will be issued.

3.1 ALGORITHM EMPLOYED

There are numerous algorithms that come under Machine Learning technology for face Recognition. Out of which KNN algorithm is among one of the simplest algorithms for Regression and Classification in Supervised Learning. For other algorithms that require more dataset whereas in KNN it requires less amount of dataset and it is also called as memory based because the way it learns is just storing the representations of training samples and also a bounding box is drawn around the detected face.

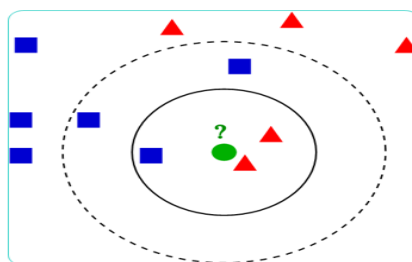


Fig -9: KNN Classification

4. CONCLUSION

Our project exhibits its better performance in the given task .Furthermore it can be used in various places which requires high security .In International Border Crossing, various security mechanisms are deployed to ensure secure travel for the travellers. In Spite of those measures some intruders get their way with fake documents. So our project when implemented in the border crossing , provides higher security where a third party access is denied and a secure travel is made by the individuals of their own nation .

5. REFERENCES

- [1]. Dubey, Arun & Jain, Vanita. (2019). A review of face recognition methods using deep learning networks. Journal of Information and Optimization Sciences. 40. 547-558. 10.1080/02522667.2019.1582875.
- [2].Wang, Hao & Wang, Yitong & Zhou, Zheng & Ji, Xing & Li, Zhifeng & Gong, Dihong & Zhou, Jingchao & Liu, Wei. (2018). CosFace: Large Margin Cosine Loss for Deep Face Recognition.
- [3].Nakada, Masaki & Wang, Han & Terzopoulos, Demetri. (2017). AcFR: Active Face Recognition Using Convolutional Neural Networks. 35-40. 10.1109/CVPRW.2017.11.
- [4].Li, Chen & Wei, Wei & Jiaxue, Li & Song, Wei. (2016). A cloud-based monitoring system via face recognition using Gabor and CS-LBP features. The Journal of Supercomputing. 10.1007/s11227-016-1840-6.

