**DocFace: ID Document to Selfie Matching**

**Alternative Title: Face Recognition in digital documents with live image**

**Aim:**

The main aim of this project is to solve the problem of counterfeiting certificates we are proposing an digital certificate system based on block chain technology and to verify the traveler’s identity using live camera, which allows faster convergence and more generalizable representations.

**Synopsis:**

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 (selfies) in real time and with high accuracy is required. In this paper, we propose DocFace+ to meet this objective. 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.

**Existing System:**

In the existing system, Identity verification plays an important role in our daily lives. 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 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 (selfies) in real time and with high accuracy is required. After verifying a traveler’s identity by face comparison, the gate is automatically opened for the traveler to enter. For IDselfie matching, they are comparing a scanned or digital document photo.

**Problem Statement:**

* The problem of ID-selfie matching poses numerous challenges that are different from general face recognition. For typical unconstrained face recognition tasks, the main challenges are due to pose, illumination and expression (PIE) variations.
* The low quality of document photos due to image compression1 and (2) the large time gap between the document issue date and the verification date remain as the primary difficulties.

**Proposed System:**

We are proposing a certificate system based on blockchain to overcome the problem. Data are 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 based on Ethereum blockchain. This technology was selected because it is incorruptible, encrypted, and trackable and permits data synchronization. By integrating the features of blockchain, the system improves the efficiency operations at each stage. The system saves on paper, cuts management costs, prevents document forgery, and provides accurate and reliable information on digital certificates and compare user live face with verified document face.

**Modules:**

* **User Registration And Authentication**
* **User Upload Certificate**
* **Get Certificate**
* **QR Request And Response From Verification Authority**

**User Registration And Authentication:**

In this module user needs to registers into his application and a request will be sent to central board server for authentication. Unless the central board server approves the request user cannot login into his account. When central board server approves the request a key will be generated and user can login into his account.

**User Upload Certificate:**

After user login into his account he needs to upload certificates namely pan card, aadhar card, voter id, ssc certificates to central board server. Central board server will review the certificates and accepts or decline the certificates. If central board server accepts the accepts the certificate those details will be stored in E.C.S and Blockchain. If central board server declines the certificate it won’t be stored in E.C.S. or Block Chain.

**Get Certificate:**

If user needs a certificate he will send request to central board server. If central board server found the user details to be genuine he accepts the request and forward a request to E.C.S where all the certificates will be there. E.C.S. responds for the request and certificates will be provided to the user.

**QR Request and Face verification:**

If user wants to apply for any certificates he will send request to central board server and central board server will check the details and forward the request to E.C.S. E.C.S will generate the QR Code and forwarded to user via central board server. User forwards the QR code to the verifying authority and if all details are correct and face matches with live face Verifying authority will issue the document.

**Algorithm Used:**

* KNN
* RSA
* SHA-256

**Software Requirements**

* Windows 7 and above
* JDK 1.7
* J2EE
* Tomcat 7.0
* MySQL

**Hardware Requirements**

* Hard Disk : 80GB and Above
* RAM : 4GB and Above
* Processor : P IV and Above

**Technology Used**

* + - J2EE (JSP, Servlet), JavaScript, HTML, CSS, AJAX.
    - Hibernate Framework
    - MVC Pattern
    - Design Pattern

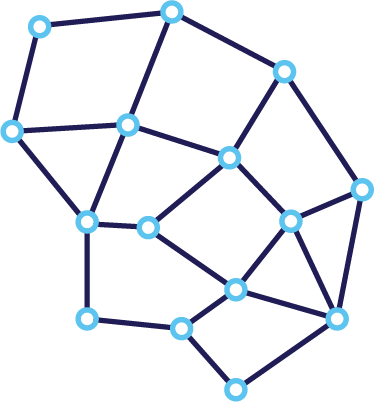
**Architecture:**



User Application



Central Board Server



Registration

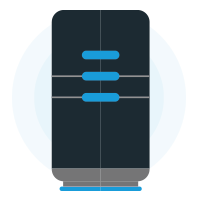
& Request

Approval

Request &

Response

Block chain



E.C.S

Upload Certificates

Upload

Certificates

Verifying

Authority

Face verification

QR Code

QR code

QR Request