

# DOCFACE+: ID DOCUMENT TO SELFIE MATCHING USING BLOCKCHAIN TECHNOLOGY

**Pramod C N<sup>1</sup>, Bhavana G<sup>2</sup>**

Student, Department of MCA, Visvesvaraya center for PG studies muddenahalli<sup>1</sup>

Assistant Professor, Department of MCA, Visvesvaraya center for PG studies muddenahalli<sup>2</sup>

**ABSTRACT:** The majority of daily activities need us to submit ID cards containing facial images, such as passports and driver's licences, to human operators in order to prove our identification. This process, however, is laborious, slow, and unreliable. An automated method is required to adapt ID document photos to real-time, highly accurate live face images (selfies). To do this, DocFace+ is recommended in this work. We first show that gradient-based optimization techniques converge slowly when many classes have small samples, which is a defining characteristic of existing ID-selfie datasets (owing to the parameter of classifier weights). To fix this problem, we propose a method known as dynamic weight imprint, which modifies the classification weights and allows for faster convergence and more universally applicable representation. Then, utilising partially shared parameters, a pair of sister networks is created to learn an unified feature representation utilizing domain-specific traits. Cross-validation on to an ID-selfie dataset reveals that DocFace+ significantly raises the true acceptance (TAR) to 95.95 0.54 percent, while InsightFace, a publicly accessible general face matching engine, only did manage a TAR of 88.78 1.30 percent at the a false acceptance rate of 0.01 percent just on challenge.

**Keywords:** Images, Face verification, Digital certificate.

## 1 INTRODUCTION

This project's primary goal is to address the issue of fake certifications. We suggest a blockchain-based digital certificate system that uses a live camera to validate the traveler's identity and enable faster convergence and much more generalizable representations. Distributed. For a number of daily activities, we must produce our identity documents—which must have face photographs—to human operators, such as passports or driver's licences. However, this procedure is time-consuming, labor-intensive, and unreliable. Therefore, a real-time, extremely precise auto was required. In this study, DocFace+ is recommended as a tool for reaching this goal. We first demonstrate that gradient-based optimization techniques converge slowly when many classes contain few samples, which is a hallmark of extant ID-selfie datasets (owing to underfitting of classifier weights). To fix this problem, all classifier weights are changed, resulting in faster convergence and more universal representations. Then, two sister networks are trained using partially shared parameters to form a single face representation using domain-specific properties. So there is an available to the public face matcher for the general public, cross-validation on to an ID selfie dataset reveals.

## 2 RELATED WORK

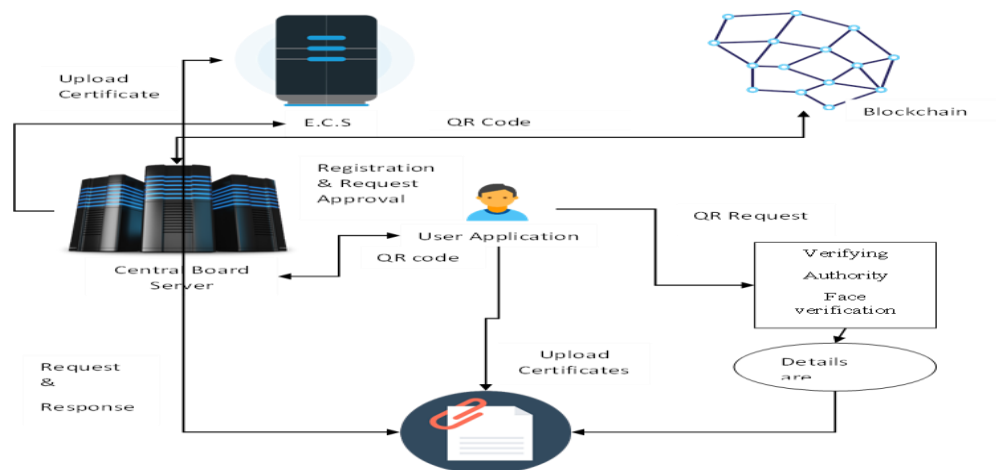
Identity verification is essential to our daily lives under the current system. For instance, we must authenticate our identities and access (security) level in order to pass through network access, physical security, or international border crossing. to prove our identification by presenting IDs featuring facial photographs to human operators, such as passports or driver's licences However, this process is labor-intensive, time-consuming, and unreliable. For matching Identification document photographs to live facial images, a real-time, highly accurate automated system is needed (selfies). The traveler's identity is confirmed through face comparison before the gate was automatically opened to allow them to pass through. They are contrasting an ID selfie with a picture of the a scanned and digital document. We suggest a blockchain-based testimony framework to solve the problem. Anyone desiring to update an internal datum must request that it should be modified simultaneously by numerous hubs because information is kept in different hubs. We created a decentralised application as well as a declaration framework on the Ethereum blockchain. This innovation is chosen since it is moral, identifiable, scrambled, and it also synchronises information. The architecture increases efficiency at each level by adding blockchain components.

**3 PRELIMINARIES**

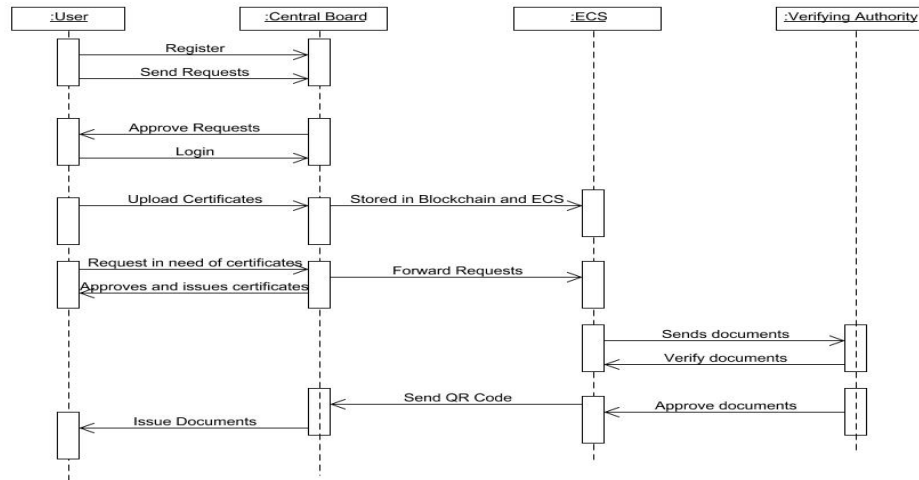
Our daily activities heavily involve confirming our personality. For instance, identity verification and entrance (security) level verification are required for access control, actual security, and cross-border communication. A simple and common solution to this issue is to compare a person's real face to the facial image presented on their ID report. For instance, movement and customs authorities look just at visa photo to confirm a traveler's character. In the US, a staff checks a customer's face or driver's licence to establish their age before letting them purchase alcohol. There are numerous situations when ID archive photos matching can be found. In any case, it is primarily managed by people who are physically present, which really is time-consuming, costly, and prone to errors. According to a poll by Sydney, Australia's identification officers, even the trained staff has trouble matching new faces to visa images, with a false acknowledgment rate of 14%. A exact & computerised framework is required to effectively match ID record photographs to selfies. Automated ID-selfie match systems can enable remote validation uses that are generally impractical, such onboarding new users inside a mobile app (by assessing their personalities on account creation) or records recovery due to password amnesia. One application scenario serves as an illustration for our ID-selfie match framework (DocFace+).

**4 PROJECT PURPOSE AND SCOPE**

The major goal of this project is to tackle certificate forgery by proposing the blockchain-based digital certificate systems and using a live camera to verify the traveler's identity, that enables convergence speed and much more generalizable representations. We offer a blockchain-based declaration framework to address the issue. Anyone desiring to update a certain inner datum must request that multiple hubs alter it simultaneously because information is kept at numerous hubs. In this regard, the structure is fairly dependable. We created a decentralised application as well as a declaration framework based on ethereum blockchain. The accuracy, recognizability, and scrambling of this technology make it ideal for synchronising information. Paper is saved, administrative costs are reduced, record forgery is avoided, accurate and trustworthy information about advanced testaments is provided, and a comparison between client live face or verified archive face is made using the system.

**5 ARCHITECTURE AND TECHNOLOGY****Fig1** Architecture of DocFace**DIAGRAM OF THE SEQUENCE**

A Sequence graph is a type of connection outline that shows how and in what order cycles interact with one another. It is a series of Message Sequence outlines, which are also known as event graphs, event landscapes, and timeframe diagrams.

**Fig2** Sequence diagram of docfac

## 5 CONCLUSION

For the purpose of comparing selfies with ID record images, a new tech called DocFace is advised. On a personal ID-selfie dataset, movement learning is the method used to refine a base model with unconstrained face correlation. Few sister networks with substantially shared-level module are employed as space explicit borders. We propose a distinct optimization technique called "dynamic weight imprinting" to address the weight-shift issue we identified while grouping or inserting learning algorithms with respect for short datasets (DWI). Prior studies have shown that the proposed system not only accelerates the loss convergent and also enhances generalisation performance. Comparing to static batch imprinting techniques demonstrates that is capable of effectively capturing the global distribution of embeddings. Additionally, the information included in the documents is protected by the Block Chain approach, which is probably the fastest and sequence.

### Future scope:

We use this system in a number of authentication sectors even though it is fully functional. The airport, government buildings, and colleges in this region have all implemented this technique for document verification. This system uses blockchain authentication technologies as well as all verification features. Future goals for this system include creating a mechanism that might utilise more industrial sites for verification industries as well as attempting to construct a mobile application that would allow uploading documents.

## REFERENCES

- [1] R. Jenkins, M. Matheson, D. R. I. Kemp, and A. White Published ONE, vol. Art. no. e103510, 9, no. 8, 2014. M. Burton, "Errors in face matching by passport authorities."
- [2] Border security and U.S. Customs (2018). Automation for Passport Control (APC). [Online]. Visit <https://www.cbp.gov/travel/uscitizens/> to access APC.
- [3] Hock a Xinjiang-based manufacturer of perimeter security gear (2018). What Is ID-Person Matching, Exactly? [Online]. Available at <http://www.xjhazj.com/xjhazj/vip doc/8380983.html>.
- [4] "A discriminative feature learning strategy for deep face recognition," by Xing, was published in Proc. 499-515 in ECCV 2016. It was written by Y. K. Zhang, Z. Li, and Y. Wen.
- [5] "A benchmark study of large-scale unconstrained face recognition," by Z. Li, published in Proc. IJCB, pp. 1-8, 2014; S. S. Liao, Z. Lei, D. Yi, and Liao.