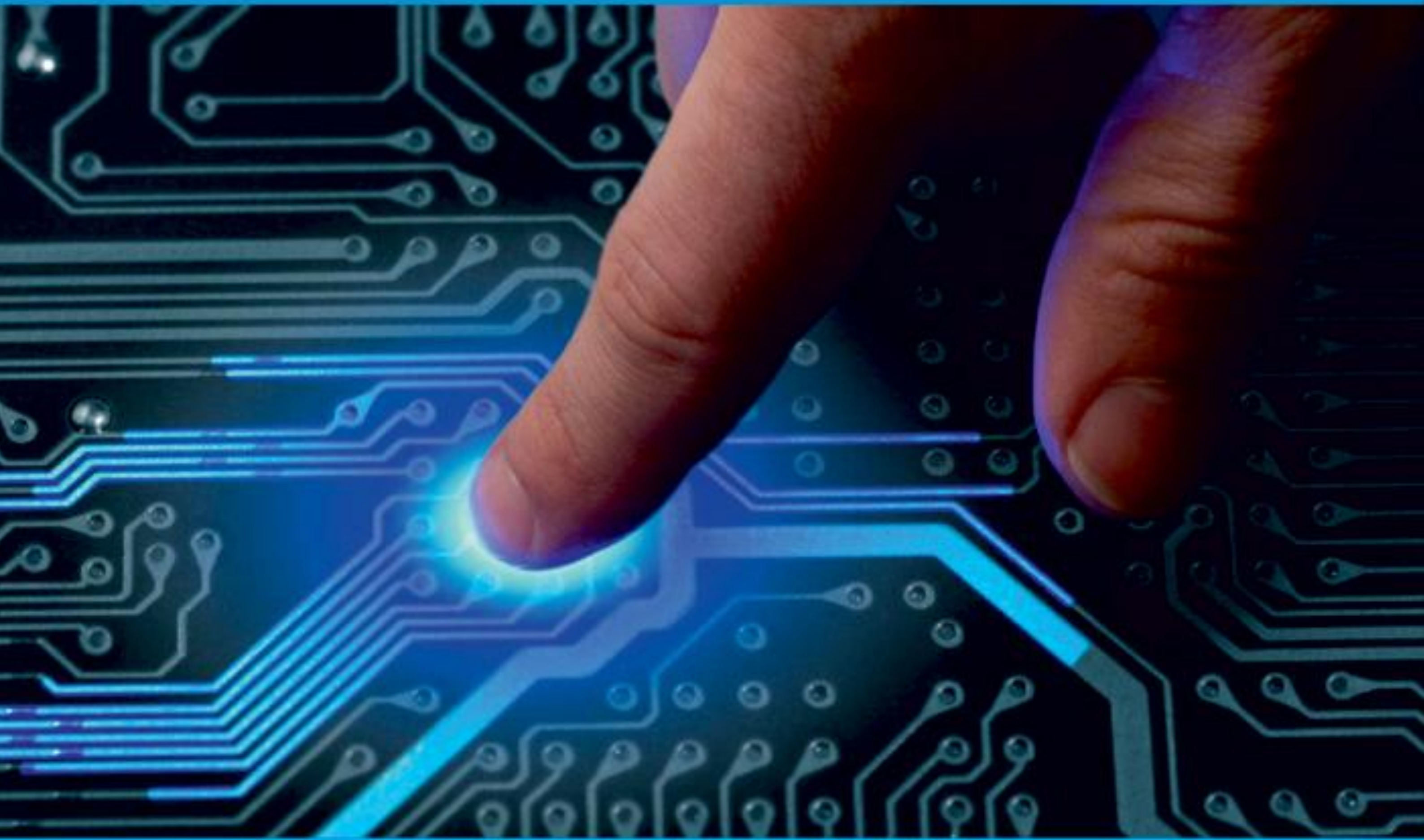
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 10, Issue 5, May 2022

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.165

Digital Documents authentication System Using Blockchain with Facial Recognition

Nihaal Singh K V[1], Raahkesh S[2], Khadar C[3], K.Gunasekaran[4]

UG Student, Dept. of CSE, Panimalar Engineering College, Tamil Nadu, India[1,2,3]

Assistant Professor, Dept. of CSE, Panimalar Engineering College, Tamil Nadu, India[4]

ABSTRACT: Innumerable activities in our day-to-day life necessitate us to verify our identity by showing Identity proof documents containing face images, such as Aadhaar and passports, to individual operators. However, this process is labor-intensive, time-consuming, and unreliable. As such, an automated system for matching Identity document photographs to live face images in real-time and with high accuracy is required. In this paper, we propose Digital Documents Authentication System using Blockchain with Facial Recognition to meet this objective. Firstly, we 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 Identity Document-selfie datasets. To overcome this drawback, we put forward a dynamic weight imprinting method to update the classifier weights, allowing faster convergence and more generalizable representations. Secondly, a pair of sibling networks with partially shared parameters are trained to learn a unified face representation with domain-specific parameters.Cross-validating an Identity Document-selfie dataset reveals that a publicly available general face matcher (Insight Face) only achieves a true accept rate (TAR) of 88.78 ± 1.30% at a false accept rate of 0.01% on the problem, Our Digital Document Authentication System improves the TAR to 95.95 ± 0.54%.

I.INTRODUCTION

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. 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. For example, immigration and customs officials look at the passport photo to confirm a traveler’s identity. Clerks at supermarkets in the United States look at the customer’s face and driver’s license to check his/her age when the customer is purchasing alcohol. Instances of ID document photo-matching can be found in numerous scenarios. However, it is primarily conducted by humans manually, which is time-consuming, costly, and prone to operator errors.

A study pertaining to the passport officers in Sydney, Australia, shows that even the trained officers perform poorly in matching unfamiliar faces to passport photos, with a 14% false acceptance rate. Therefore, an accurate and automated system for efficient matching of ID document photos to selfies* is required. In addition, automated ID-selfie matching systems also enable remote authentication applications that are otherwise not feasible, such as onboarding new customers in a mobile app (by verifying their identities for account creation), or account recovery in the case of forgotten passwords. One application scenario of our ID-selfie matching system is illustrated.

A number of automated ID-selfie matching systems have been deployed at international border crossings. Due to an increasing number of travelers to Australia, the Australian government introduced SmartGate at most of its international airports as an electronic passport check for ePassport holders. To use the SmartGate, travelers only need to let a machine read their ePassport chips containing their digital photos and then capture their face images using a camera mounted at the SmartGate. After verifying a traveler’s identity by face comparison, the gate is automatically opened for the traveler to enter Australia.

In addition to international bordercontrol, some businesses are utilizing face recognition solutions to ID document verification for online services.

II.RELATED WORK

Numerous activities in our daily life, including purchases, travels and access to services, require us to verify who we are by showing ID documents containing face images, such as passports and driver licenses. An automatic system for matching ID document photos to live face images in real time with high accuracy would speed up the verification process and reduce the burden on human operators. In this paper, we propose a new method, DocFace, for ID document photo matching using the transfer learning technique. We propose to use a pair of sibling networks to learn domain specific parameters from heterogeneous face pairs. Cross validation testing on an ID-Selfie dataset shows that while the best CNN-based general face matcher only achieves a TAR=61.14% at FAR=0.1% on the problem, the DocFace improves the TAR to 92.77%. Experimental results also indicate that given sufficiently large training data, a viable system for automatic ID document photo matching can be developed and deployed.

Three main tasks of face recognition may be named: “document control”, “access control”, and “database retrieval”. The term “document control” means the verification of a human by comparison his/her actual camera image with a document photo. Access control is the most investigated task in the field. Such systems compare the portrait of a tested person with photos of people who have access permissions to joint used object. The last task arises when it is necessary to determine name and other information about a person just based on his/her one casual photo. Because of great difference between the tasks there is not a universal approach or algorithm for face recognition [1-4]. We tested several methods for mentioned above tasks: geometric approach, elastic matching and neuron nets. Summary of our experiments are described below.

III.SYSTEM ANALYSIS

EXISTING SYSTEM

In the existing system, Digital locker commonly known as DigiLocker is a digital document wallet that stores an individual’s documents and keeps them safe. Individuals can access their documents which are stored in DigiLocker at any time. This application provides a cloud storage service to the documents issued by the Government of India.

However, Only Aadhar cardholders can use the DigiLocker app- For making an account on DigiLocker, it is necessary to provide the Aadhar number of an individual.

Security concerns- Recently, the DigiLocker team confirmed that there was a vulnerability with the account data. DigiLocker has admitted that nearly 3.68 crores were at risk and anyone having the username of the account can access the account’s documents. The hackers don’t even require a PIN or password to access the account.

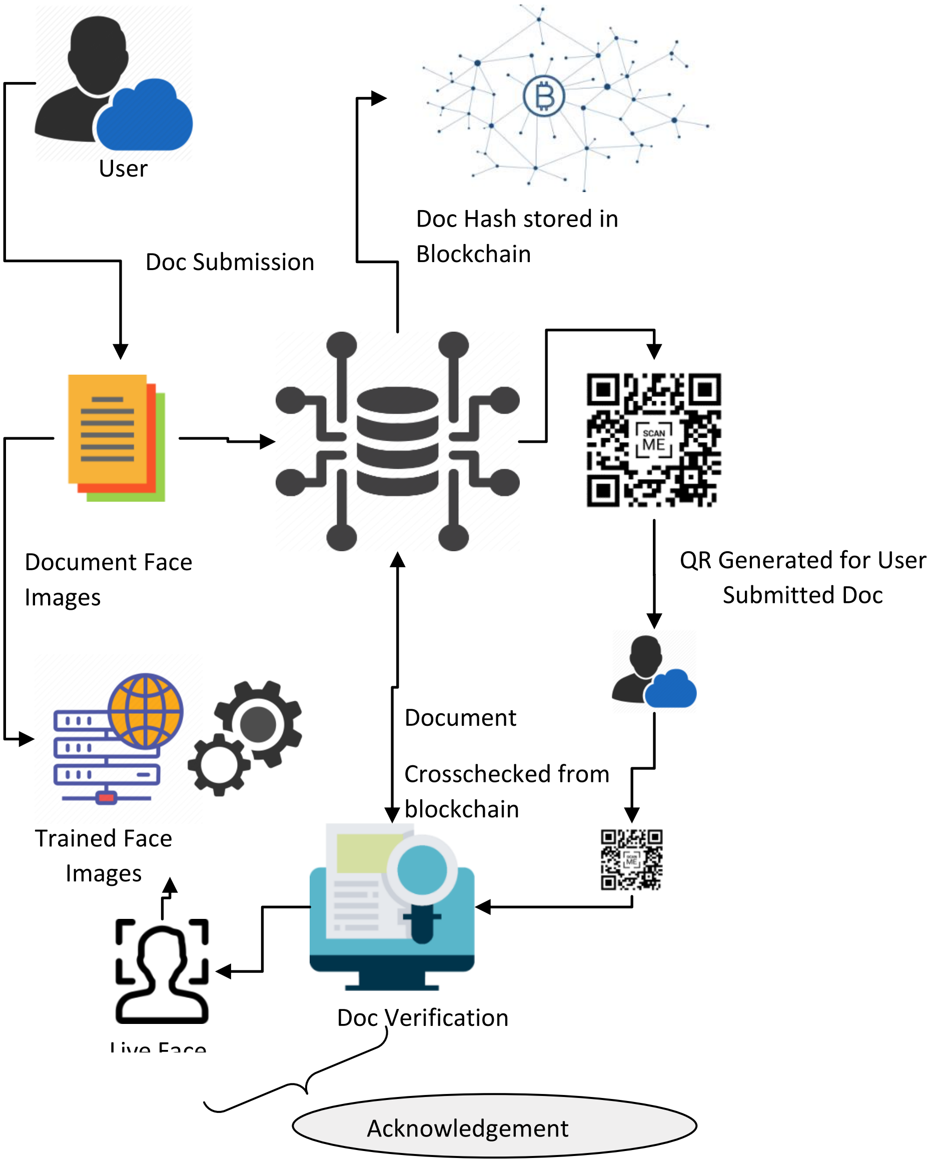
IV.PROPOSED SYSTEM

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. Byintegrating 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.

| DOI: 10.15680/IJIRCCE.2022.1005029|

V.ARCHITECTURE OVERVIEW



ARCHITECTURE DIAGRAM

VI.ALGORITHM DESCRIPTION

ALGORITHM USED

- KNN
- RSA
- SHA-25

K-NEAREST NEIGHBOUR:

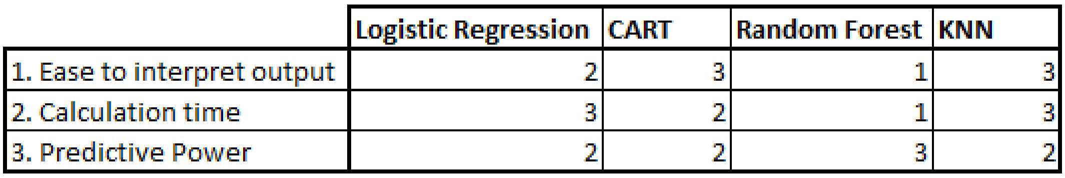
KNN can be used for both classification and regression predictive problems. However, it is more widely used in classification problems in the industry. To evaluate any technique we generally look at 3 important aspects:

1. Ease to interpret output

2. Calculation time

3. Predictive Power

Let us take a few examples to place KNN in the scale:

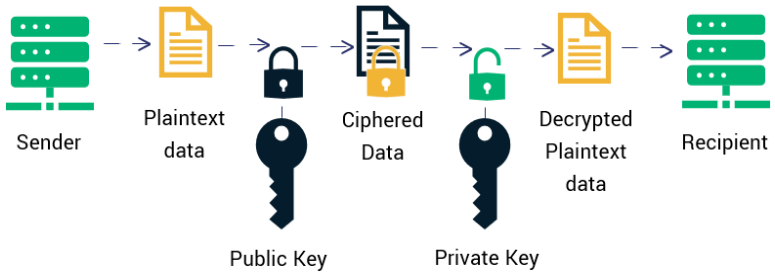


	Logistic Regression	CART	Random Forest	KNN
1. Ease to interpret output	2	3	1	3
2. Calculation time	3	2	1	3
3. Predictive Power	2	2	3	2

KNN algorithm fairs across all parameters of considerations. It is commonly used for its easy of interpretation and low calculation time.

RSA

RSA algorithm is asymmetric cryptography algorithm. Asymmetric actually means that it works on two different keys i.e. Public Key and Private Key. As the name describes that the Public Key is given to everyone and Private key is kept private.



SHA-256

SHA 256 is a part of the SHA 2 family of algorithms, where SHA stands for Secure Hash Algorithm. Published in 2001, it was a joint effort between the NSA and NIST to introduce a successor to the SHA 1 family, which was slowly losing strength against brute force attacks.

The significance of the 256 in the name stands for the final hash digest value, i.e. irrespective of thesize of plaintext/cleartext, the hash value will always be 256 bits.

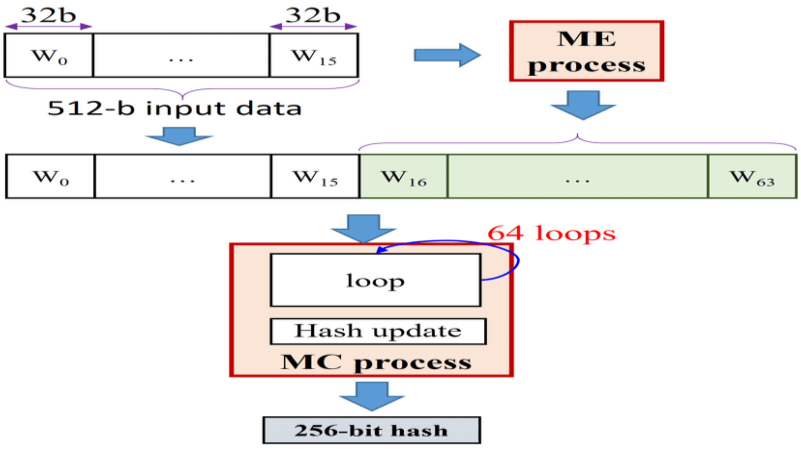


FIG 7.1.3

VI.TEST CASES & REPORTS

S.no	Action	Inputs	Expected Result	Actual Result	Testcase: Pass/fail
1	Launch Application	Click button	Home page	Home page	Pass
2	Enter correct email, name and password	Enter email id, Password andName	Login successful	Login successful	Pass
3	Enter wrong name and password	Enter wrong username and password	Prompts invalid username and password	Prompts invalid username and password	Pass
4	Submit button	Click button	Login successful	Login successful	Pass

Test Case: Registration   Test Priority: High

| DOI: 10.15680/IJIRCCE.2022.1005029|

VII.CONCLUSION

Cross-validating an Identity Document-selfie dataset reveals that a publicly available general face matcher (Insight Face) only achieves a true accept rate (TAR) of 88.78 ± 1.30% at a false accept rate of 0.01% on the problem, Our Digital Document Authentication System improves the TAR to 95.95 ± 0.54%.

REFERENCES

[1] D. White, R. I. Kemp, R. Jenkins, M. Matheson, and A. M. Burton, “Passport officers’ errors in face matching,” *PLoS ONE*, vol. 9, no. 8, 2014, Art. no. e103510.
[2] Wikipedia. (2018). *Australia Smartgate*. [Online].
Available: https://en.wikipedia.org/wiki/SmartGate
[3] Wikipedia. (2018). *Epassport Gates*. [Online].
Available: https://en. wikipedia.org/wiki/EPassport_gates
[4] U.S. Customs and Border Protection. (2018). *Automated Passport Control (APC)*. [Online]. Available: https://www.cbp.gov/travel/uscitizens/apc
[5] Xinjiang Heng An Perimeter Security Equipment Company. (2018). *What Is ID-Person Matching?* [Online]. Available: http://www.xjhazj.
com/xjhazj/vip_doc/8380983.html
[6] Jumio. (2018). *Netverify ID Verification*. [Online]. Available: https://www.jumio.com/trusted-identity/netverify.
[7] Mitek. (2018). *Mitek ID Verification*. [Online]. Available: https://www.miteksystems.com/mobile-verify
[8] G. B. Huang, M. Ramesh, T. Berg, and E. Learned-Miller, “Labeled faces in the wild: A database for studying face recognition in unconstrained environments,” Univ. Massachusetts, Amherst, MA, USA, Rep. 07-49, Oct. 2007 V. Starovoitov, D. Samal, and B. Sankur, “Matching of faces in camera images and document photographs,” in *Proc. ICASSP*, 2000, pp. 2349–2352. [10] T. Bourlai, A. Ross, and A. Jain, “On matching digital face images against scanned passport photos,” in *Proc. IEEE Int. Conf. BiometricsIdentity Security (BIDS)*, 2009, pp. 1–10.
[11] T. Bourlai, A. Ross, and A. K. Jain, “Restoring degraded face images: A case study in matching faxed, printed, and scanned photos,” *IEEETrans. Inf. Forensics Security*, vol. 6, no. 2, pp. 371–384, Jun. 2011.
[12] V. V. Starovoitov, D. I. Samal, and D. V. Briliuk, “Three approaches for face recognition,” in *Proc. Int. Conf. Pattern Recognit. Image Anal.*, 2002, pp. 707–711.
[13] Y. Shi and A. K. Jain, “DocFace: Matching ID document photos to selfies,” in *Proc. BTAS*, 2018, pp. 1–8.
[14] X. Zhu *et al.*, “Large-scale bisample learning on ID vs. spot face recognition,” *arXiv:1806.03018*, 2018.
[15] Q. Cao, L. Shen, W. Xie, O. M. Parkhi, and A. Zisserman, “VGGFace2: A dataset for recognising faces across pose and age,” in *Proc. IEEE Conf.Autom. Face Gesture Recognit.*, 2018, pp. 1–8.
[16] A. Krizhevsky, I. Sutskever, and G. E. Hinton, “ImageNet classification with deep convolutional neural networks,” in *Proc. NIPS*, 2012, pp. 1–9.
[17] Y. Taigman, M. Yang, M. Ranzato, and L. Wolf, “DeepFace: Closing the gap to human-level performance in face verification,” in *Proc. CVPR*, 2014, pp. 1701–1708.
[18] Y. Sun, Y. Chen, X. Wang, and X. Tang, “Deep learning face representation by joint identification-verification,” in *Proc. NIPS*, 2014, pp. 1988–1996.

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details