IJETIR

ISSN (Online) 2583-0554

International Journal of Emerging Technologies and Innovative Research (IJETIR)

Volume 4, Issue 6, June 2024

Impact Factor: 5.731

AI based ID Card Fraud Detection using Deep Adversarial Network

Sowmiya. K[1] and Dr. D. R. Krithika[2]

MCA Student, Department of Computer Applications[1]

Assistant Professor, Department of Computer Applications[2]

22304239@vistas.ac.in and krithika.scs@velsuniv.ac.in

Vels Institute of Science, Technology & Advanced Studies (VISTAS), Chennai, Tamil Nadu, India

Abstract: *ID cards are official documents issued by government authorities or institutions to verify a person's identity. Educational certificates are official documents awarded by educational institutions, such as schools, colleges, and universities, to individuals who have successfully completed a specific program of study. They typically include the individual's name, photograph, date of birth, a unique identification number, the name of the institution, the degree or qualification earned, the date of completion, and sometimes additional details like the program of study or academic honours Both documents play important roles in various aspects of an individual's life, including employment, education, and official identification. Presentation attacks on ID cards and educational certificates encompass a range of deceptive tactics employed by individuals with malicious intent to undermine the authentication and validation processes associated with these documents. These attacks can have diverse objectives, from gaining unauthorized access to secured areas to securing employment or admissions under false pretences. In the case of ID cards, common presentation attacks involve forgery, counterfeiting techniques, photo substitution, tampering, and even the pretext of having lost one's ID card. On the other hand, educational certificate presentation attacks include utilizing diplomas from diploma mills, falsifying academic transcripts, resume fraud, and even compromising credential verification systems*

Keywords: EC (Encumbrance Certificate)

I. INTRODUCTION

An identity document (also called a piece of identification or ID, or colloquially as papers) is any document that may be used to prove a person's identity. If issued in a small, standard credit card size form, it is usually called an identity card (IC, ID card, citizen card), or passport card. Some countries issue formal identity documents, as national identification cards which may be compulsory or non-compulsory, while others may require identity verification using regional identification or informal documents. When the identity document incorporates a person's photograph, it may be called photo ID. In the absence of a formal identity document, a driver's license may be accepted in many countries for identity verification. Some countries do not accept driver's licenses for identification, often because in those countries they do not expire as documents and can be old or easily forged. Most countries accept passports as a form of identification. Some countries require all people to have an identity document available at any time. Many countries require all foreigners to have a passport or occasionally a national identity card from their home country available at any time if they do not have a residence permit in the country.The identity document is used to connect a person to information about the person, often in a database. The photo and the possession of it is used to connect the person with the document. The connection between the identity document and information database is based on personal information present on the document, such as the bearer's full name, age, birth date, address, an identification number, card number, gender, citizenship and more

IJETIR
ISSN (Online) 2583-0554
International Journal of Emerging Technologies and Innovative Research (IJETIR)
Volume 4, Issue 6, June 2024
Impact Factor: 5.731

II. LITERATURE SURVEY

This paper proposes a deep learning framework for detecting fake biometric data, including ID card images[1]. This survey paper provides an overview of adversarial machine learning techniques applied in various cybersecurity domains, including fraud detection[2]. This study explores deep learning techniques for detecting forged documents, including educational certificates and ID cards[3]. This research focuses on using convolutional neural networks (CNNs) for detecting forged ID cards[4]. This paper presents a deep learning approach specifically tailored for detecting fraudulent educational certificates[5]. This comprehensive survey paper provides insights into adversarial attacks and defense mechanisms in deep learning[6]. This review paper offers a comprehensive examination of deep learning-based fraud detection systems across different domains[7].

III. IMPLEMENTATION

Fig:1 ADMIN LOGIN

In this fig we need to create a new admin login and password

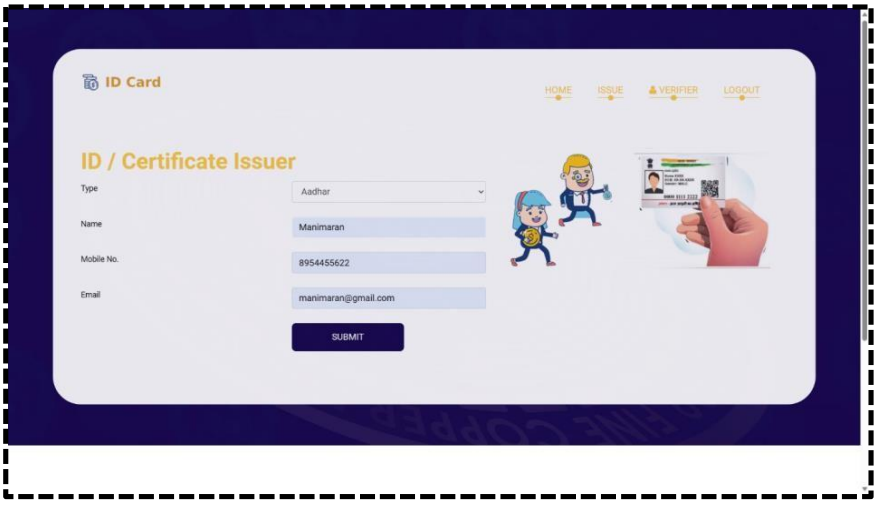

Fig:2 PERSONAL DETAILS

In this fig we need to enter the personal details like name ,mobile no, email etc…

IJETIR
ISSN (Online) 2583-0554
International Journal of Emerging Technologies and Innovative Research (IJETIR)
Volume 4, Issue 6, June 2024
Impact Factor: 5.731

Fig:3 SELECT FILE

In this fig the shown certificates details should be uploaded.

Fig:4 RPN FACE DETECTION

Then,The RPN face detection process held.

IJETIR
ISSN (Online) 2583-0554
International Journal of Emerging Technologies and Innovative Research (IJETIR)
Volume 4, Issue 6, June 2024
Impact Factor: 5.731

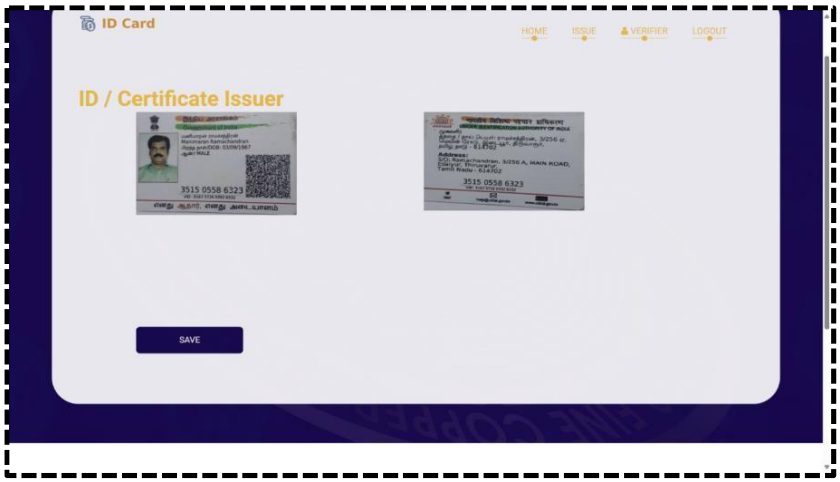

Fig:5 FILE SAVE

After the detection progress happen the document is saved now.

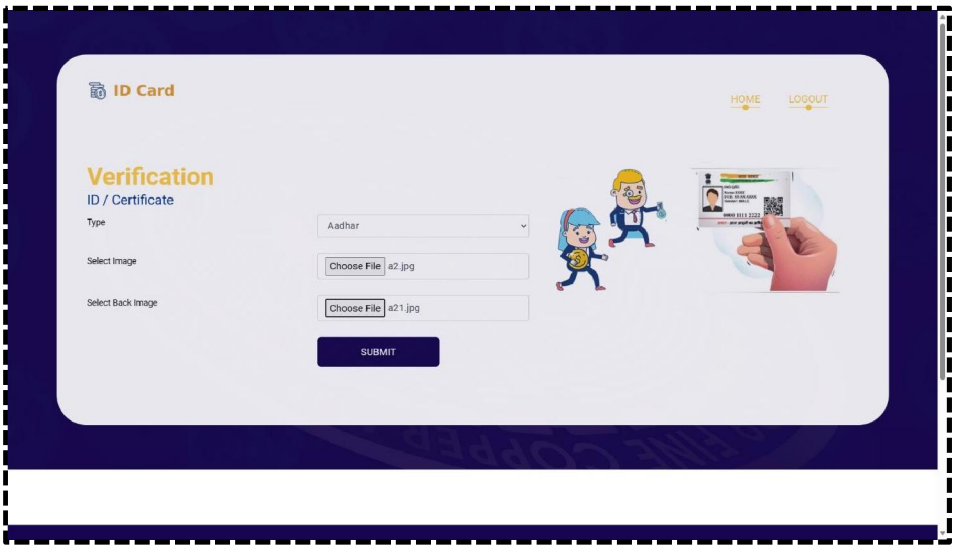

Fig:6 UPLOAD FILE(2)

Now again we need to upload a new certificate.

IJETIR
ISSN (Online) 2583-0554
International Journal of Emerging Technologies and Innovative Research (IJETIR)
Volume 4, Issue 6, June 2024
Impact Factor: 5.731

Fig:7 VERFICATION

Now it verify the both certificates like the face is matched and text is matched or not…

Fig:8 RESULT

This layout shows the certificate face and text information is matched(Aadhar card is genuine).

IV. CONCLUSION

The project marks a milestone in the domain of document verification. Through the integration of deep adversarial networks and Tesseract OCR, the system has demonstrated an impressive ability to identify and counter various presentation attacks, including Bona Fide, Composite, Print, and Screen attacks. The project's success lies in its comprehensive approach, utilizing advanced technologies to discern subtle discrepancies in documents that may elude traditional methods. One of the project's notable achievements is the incorporation of deep adversarial networks, enhancing the accuracy of fraud detection by recognizing nuanced variations in presented documents.

Additionally, the integration of Tesseract OCR has played a pivotal role in ensuring precise extraction of textual information, contributing to the overall reliability of the document verification process. Despite the successes, the project acknowledges the existence of certain challenges, such as identified bugs that are actively being addressed. Continuous testing and refinement are essential for ensuring a flawless deployment. Further improvements in OCR capabilities, especially in recognizing cursive fonts, are part of the ongoing efforts to enhance the system's versatility. The project's user-friendly interface, manifested in the End User Control Panel, ensures a seamless experience for generators, verifiers, and document holders. This accessibility contributes to the efficiency and effectiveness of the verification process.

REFERENCES

[1]. R. Lara, A. Valenzuela, D. Schulz, J. Tapia, and C. Busch, "Towards an efficient semantic segmentation method of ID cards for verification systems," 2021, arXiv:2111.12764.

[2]. X. Zhu et al., "Large-scale bisample learning on ID versus spot face recognition," Int. J. Comput. Vis., vol. 127, nos. 6–7, pp. 684–700, Jun. 2019.

[3]. T. Karras, M. Aittala, J. Hellsten, S. Laine, J. Lehtinen, and T. Aila, "Training generative adversarial networks with limited data," in Proc. Adv. Neural Inf. Process. Syst., vol. 33, 2020, pp. 12104–12114.

[4]. Y. Shi and A. K. Jain, "DocFace: Matching ID document photos to selfies," in Proc. IEEE 9th Int. Conf. Biometrics Theory, Appl. Syst. (BTAS), Oct. 2018, pp. 1–8.

[5]. S. Gonzalez, A. Valenzuela, and J. Tapia, "Hybrid two-stage architecture for tampering detection of chipless ID cards," IEEE Trans. Biometrics, Behav., Identity Sci., vol. 3, no. 1, pp. 89–100, Jan. 2021.