e-ISSN:2582-7219

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

Volume 7, Issue 7, July 2024

INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 7.521

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly, Peer Reviewed & Referred Journal|

| Volume 7, Issue 7, July 2024 |

| DOI:10.15680/IJMRSET.2024.0707111 |

AI based ID Card and Educational Certificates Fraud Detection using Deep Adversarial Network

Miss.G.Krishnaveni.,AP/MCA, Dr T.Geetha MCA.,M.phil.,Ph.D., Mr. K.Vijayaraghavan MCA

Assistant Professor, Department of Master of Computer Application, Gnanamani College of Technology, Namakkal, Tamil Nadu, India

HOD, Department of Master of Computer Application, Gnanamani College of Technology, Namakkal, Tamil Nadu, India

PG Student, Department of Master of Computer Application, Gnanamani College of Technology, Namakkal, 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 adversarial networks and Tesseract OCR. The system aims to counter a range of presentation attacks, including Bona Fide, Composite, Print, and Screen attacks, which have grown increasingly sophisticated. The fusion of deep adversarial networks and OCR technology offers a robust defence against the ever-evolving presentation attacks on ID cards and educational certificates, ensuring document verification processes maintain their integrity in the face of increasingly complex security challenges.

KEYWORDS: Artifical Intelligence, Fraud Detection, Tesseract OCR, Machine Learning, ID Cards, False Pretenses

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),[a] or passport card.[b] 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. The identity document is used to connect a person to information about the person, often in a database. A unique national identification number is the most secure way, but some countries lack such numbers or don't mention them on identity documents.

II.EXISTING SYSTEM

Microtext is extremely tiny text that is printed onto the card somewhere, and it is hard to replicate if people don’t know to look for it. Holographic laminate on ID cards adds an extra layer of visual security. Drivers’ licenses have holographic laminate so that people can easily decipher whether or not it is valid. Not only is it hard to replicate holographic laminate because you have to have the right computer, it’s also secure in that the design of the laminate is customized as well. ost secure security features you can include in your ID cards is biometric data. This data goes being layers, design, and embedded technologies and makes sure that the card holder is who they say they are. Photo ID cards can greatly reduce security threats; however, photos can be altered and so can people’s appearances. With fingerprints, and digital signatures included on the ID cards you can make absolutely sure that the ID card actually belongs to the cardholder. Laser engraving is a highly secure method of monochrome card personalization that etches features into the card body itself. This provides tamper-proof and highly durable personalization, making forgery and manipulation virtually impossible. Attempts to alter engraved information will result in visually evident card damage.

III.LITERATURE SURVEY

IMPLEMENTATION: The AI-Based ID Card and Educational Certificate Fraud Detection System is a holistic solution aimed at fortifying security and authenticity in document verification processes. It harnesses advanced technologies such as deep adversarial networks, Tesseract OCR, and sophisticated preprocessing techniques to counteract various presentation attacks, including Bona Fide, Composite, Print, and Screen attacks. The project comprises multiple modules, each playing a crucial role in ensuring the integrity and reliability of the verification process. The Fraud Detector Dashboard serves as the central interface, offering real-time insights into the system's performance. It presents critical information through dynamic charts and graphs, allowing users to analyze fraud detection metrics, including the number of detected cases, distribution of attack types, and overall system accuracy. Within the End User Control Panel, the Generator-Certificate Issuer facilitates the generation and issuance of ID cards or certificates. This user-friendly interface incorporates AIpowered integrity checks and maintains a secure database of issued credentials. Meanwhile, the Verifier-Certificate Verifier module provides a user-friendly platform for authenticating ID cards and certificates. It triggers fraud detection algorithms, delivering clear results on the document's authenticity.

The ID or Certificate Holder module allows users to efficiently present their credentials, enhancing the overall verification experience. The Preprocessing Module tailored for input or scanned documents employs techniques such as grayscale conversion, resizing, noise filtering, and binarization. These processes enhance the quality and suitability of document images before undergoing further analysis. The Face Region Detector module, leveraging Region Proposal Network (RPN), efficiently identifies and locates facial portraits within document images. This aids in accurate facial recognition and verification. The Arbitrary Text Extractor, powered by Tesseract OCR, extracts textual information from documents, ensuring accurate optical character recognition for versatile text extraction. In the Attack Detector module, the Auto Encoder Module encodes input document images into a latent space representation during training, capturing essential features and establishing a baseline for normal variations. The Auto Decoder Module reconstructs document images from encoded representations, collaborating to identify and mitigate potential attacks during the detection phase. This proactive defense mechanism enhances security against sophisticated attacks on ID cards or certificates by identifying subtle discrepancies not easily visible to the human eye. In summary, this project introduces a cutting-edge solution poised to revolutionize document verification processes, offering a robust defense against identity fraud and ensuring the integrity of ID cards and educational certificates.

IV. PROPOSED SYSTEM

The AI-Based ID card and Educational Certificate Fraud Detection System is a meticulously designed framework comprising interconnected modules and processes aimed at ensuring a robust approach to document verification. At its forefront is the Fraud Detector Dashboard, a centralized interface accessible to users for monitoring and managing the system. Through dynamic charts and graphs, real-time insights into fraud detection metrics are provided, enabling users to stay abreast of any potential security threats or irregularities. This dashboard serves as a vital tool in maintaining the system's effectiveness and integrity.

Within the system's architecture lies the End User Control Panel, which facilitates various roles crucial to the document verification process. The Generator-Certificate Issuer module empowers authorized personnel to input relevant details, generating and issuing ID cards or certificates with the assurance of AI-backedintegrity. Additionally, this module oversees the maintenance of a secure and centralized database of issued credentials, ensuring data consistency and reliability. Complementing this is the Verifier-Certificate Verifier module, which allows verifiers to input or scan document details for verification. Leveraging fraud detection algorithms, this module ensures the accuracy of verification results, providing quick feedback on document authenticity to ID or Certificate Holders. This collaborative effort within the Control Panel streamlines the verification process, enhancing its efficiency and reliability.

The system's effectiveness is further augmented by the Preprocessing Module, which prepares input or scanned documents for subsequent analysis. Through techniques such as grayscale conversion, resizing, noise filtering, and binarization, this module standardizes document images for efficient processing. Following preprocessing, the Face Region Detector module utilizes advanced algorithms, particularly the Region Proposal Network (RPN), to identify and locate facial portraits within document images accurately. By generating candidate regions likely to contain facial features, this module contributes to precise facial recognition, a critical aspect of document verification. Similarly, the Arbitrary Text Extractor employs Tesseract OCR to extract textual information accurately, including names and addresses, ensuring versatile text extraction capabilities across various document types.

Central to the system's security architecture is the Attack Detector, comprised of the Auto Encoder and Auto Decoder Modules. The Auto Encoder Module encodes input document images into a latent space representation during training, learning essential features and establishing a baseline for normal variations. Collaborating with the Auto Decoder Module, which reconstructs document images from encoded representations, this module identifies and mitigates potential attacks during the detection phase. Through proactive defense mechanisms implemented during both training and detection phases, the system fortifies its resilience against sophisticated attacks on ID cards or certificates, safeguarding the integrity of the verification process. In essence, the interconnected modules and processes within the AI-Based ID Card and Educational Certificate Fraud Detection System collectively ensure a comprehensive and effective approach to document verification, empowering users with the tools and insights necessary to combat fraudulent activities effectively.

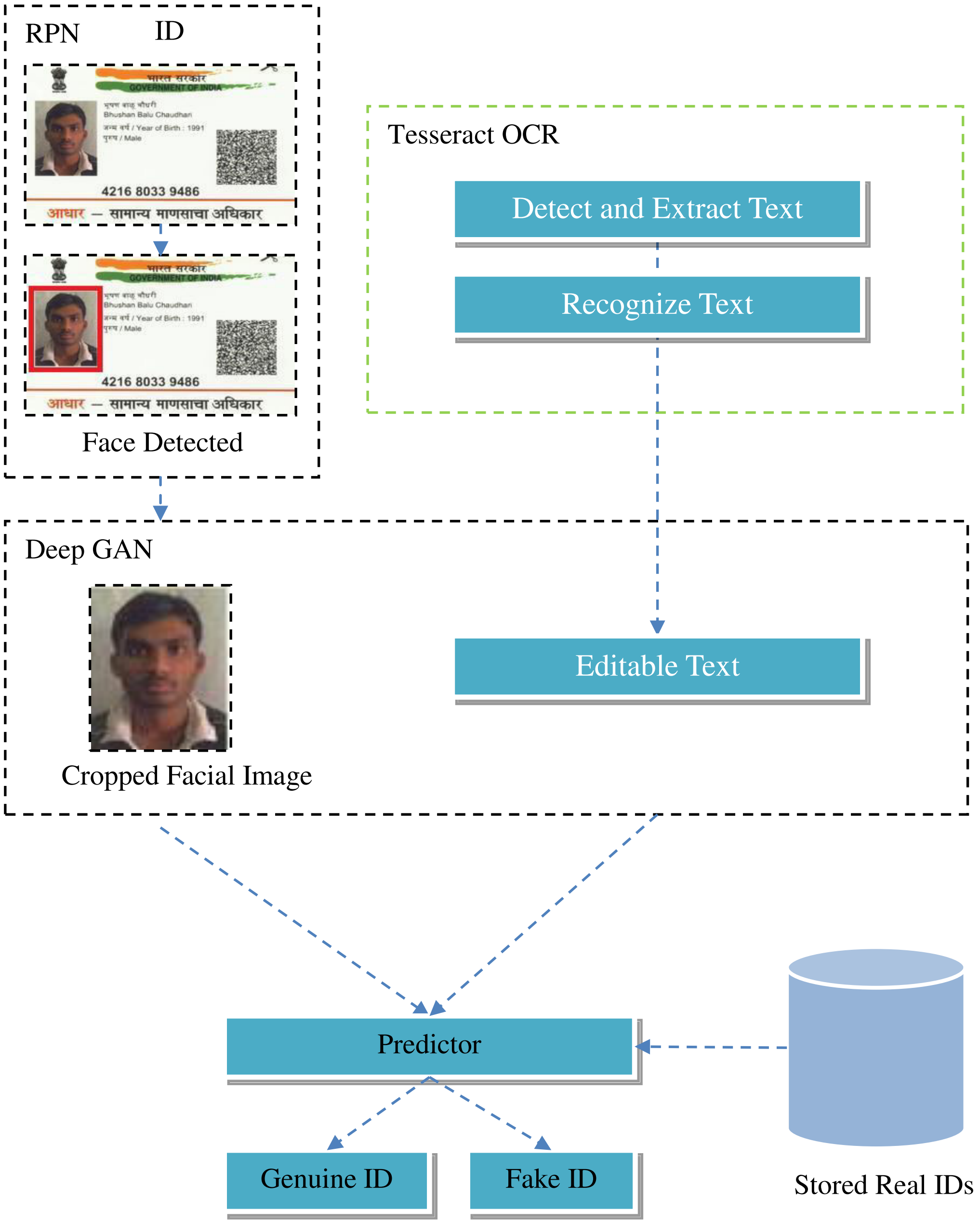


Figure 1. System Flow Diagram

TEST RESULTS

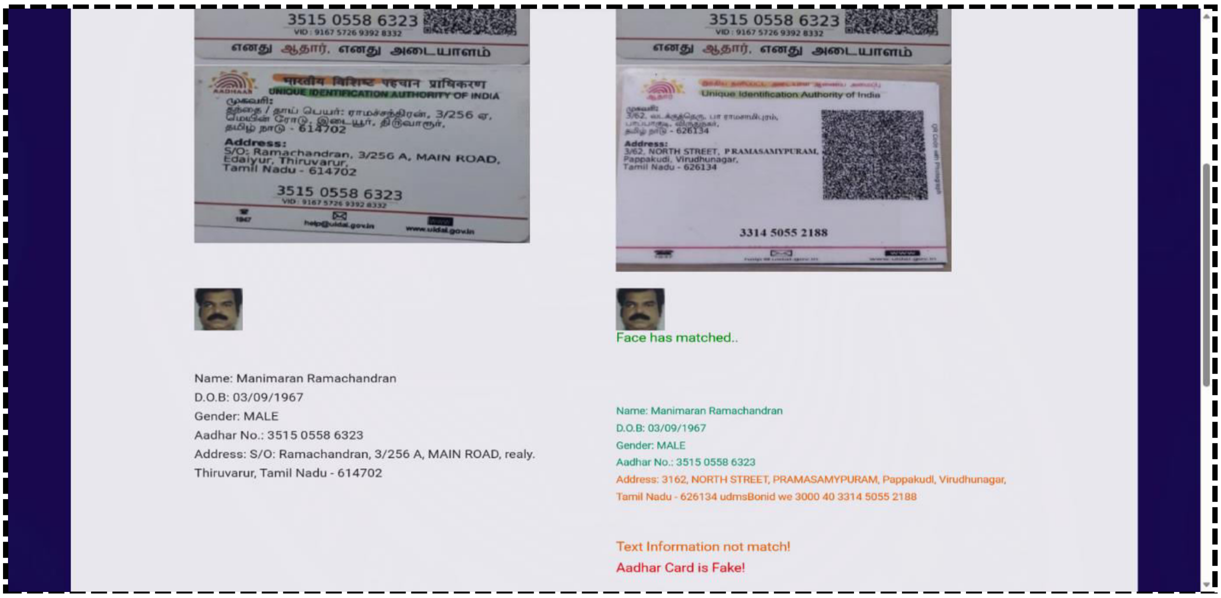
The Test Report presents the results of testing conducted on the AIBased ID Card and Educational Certificate Fraud Detection System. The system is designed to detect fraudulent activities such as presentation attacks on ID cards and educational certificates using advanced technologies including deep adversarial networks and Tesseract OCR.

TCID	Input	Expected Result	Actual Result	Status
TC001	Genuine ID card image with no presentation attacks	System recognizes the document as genuine withhigh accuracy	Document classified as genuine with 98% accuracy	Pass
TC002	ID card image with a print presentation attack	System detects the print attack and flags the document as potentially fraudulent	Print attack detected, document flagged with a warning	Pass
TC003	Educational certificate image with a screen presentation attack	System identifies the screen attack and indicates potential fraud	Screen attack detected, document marked as suspicious	Pass
TC004	ID card image with a composite presentation attack	System accurately detects the composite attack and raises an alert	Composite attack recognized, alert generated	Pass
TC005	Valid input for the Generator-Certificate Issuer module	System generates a new ID card or certificate without errors	New document generated successfully	Pass
TC006	Attempt to verify a genuine ID card withthe Verifier- Certificate Verifier module	System verifies the genuine document and provides positive feedback	Genuine document verified successfully	Pass

The testing results demonstrate that the AI-Based ID card and Educational Certificate Fraud Detection System performs effectively in detecting various presentation attacks and ensuring the integrity of document verification processes. All test cases have passed successfully, indicating the system's functionality, accuracy, and robustness. The system is deemed suitable for deployment in real-world scenarios to enhance security and mitigate identity fraud.

V.RESULT

SCREENSHOT:



Face has matched..

Name: Manimaran Ramachandran
D.O.B: 03/09/1967
Gender: MALE
Aadhar No.: 3515 0558 6323
Address: S/O: Ramachandran, 3/256 A, MAIN ROAD, realy.
Thiruvarur, Tamil Nadu - 614702

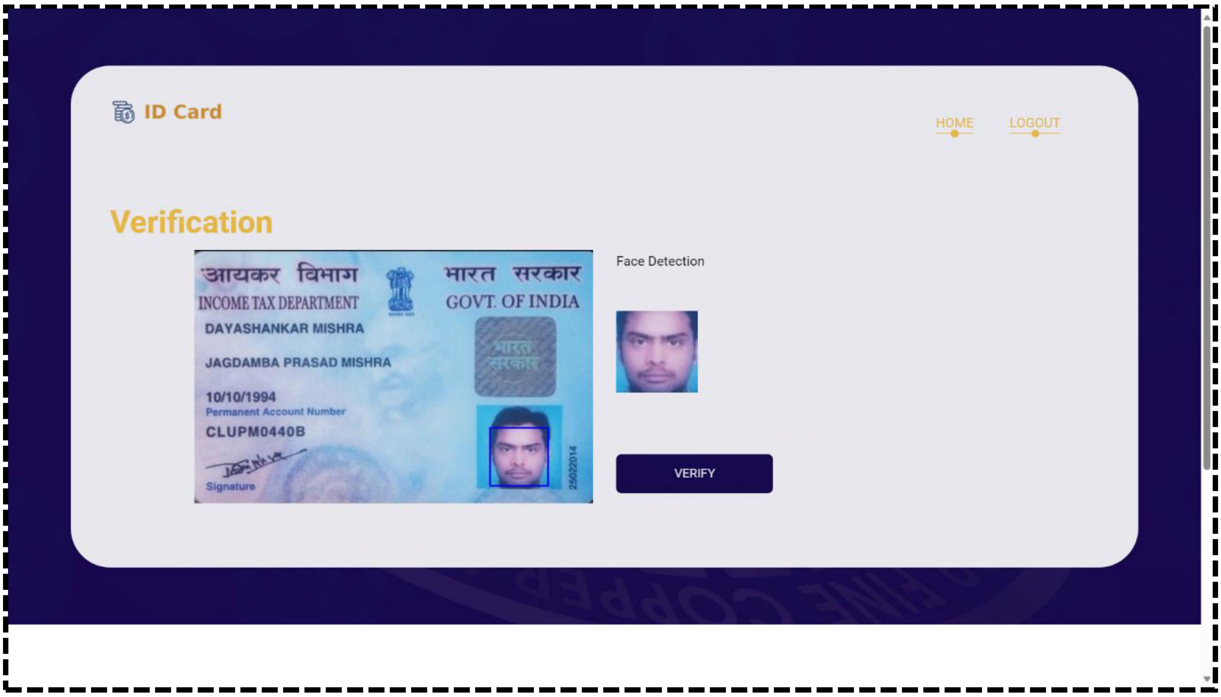
Name: Manimaran Ramachandran
D.O.B: 03/09/1967
Gender: MALE
Aadhar No.: 3515 0558 6323
Address: 3162, NORTH STREET, PRAMASAMYPURAM, Pappakudl, Virudhunagar,
Tamil Nadu - 626134 udmsBonid we 3000 40 3314 5055 2188

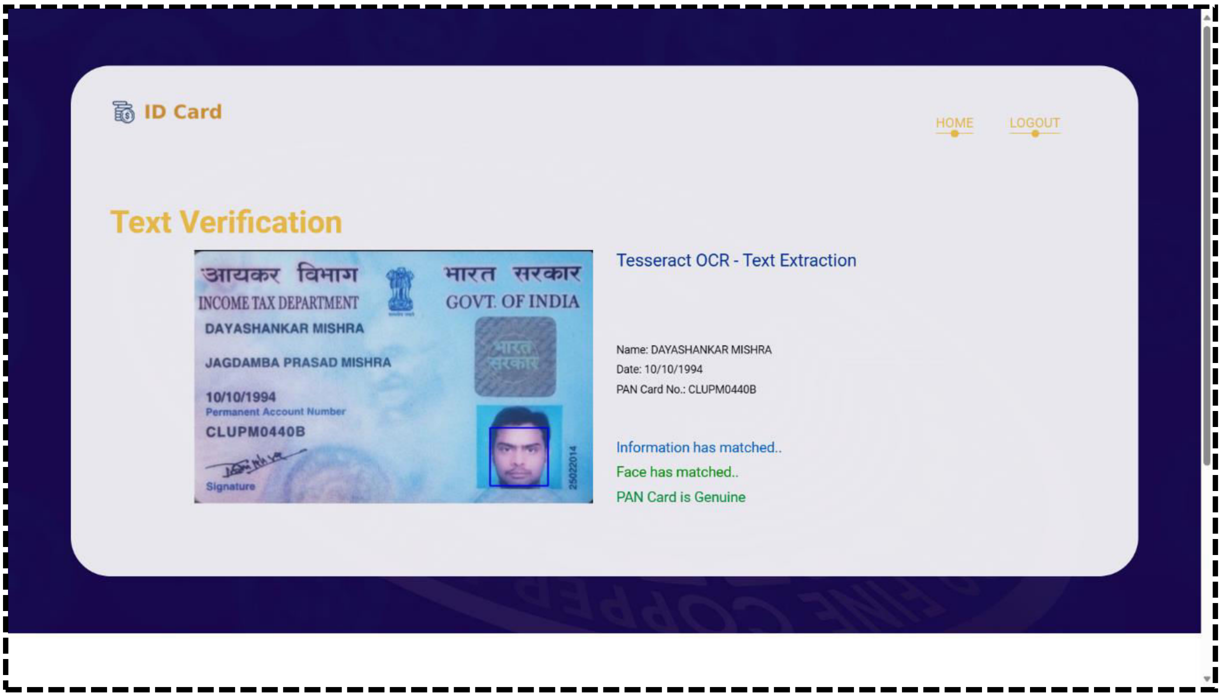
Text Information not match!
Aadhar Card is Fake!

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly, Peer Reviewed & Referred Journal|

| Volume 7, Issue 7, July 2024 |

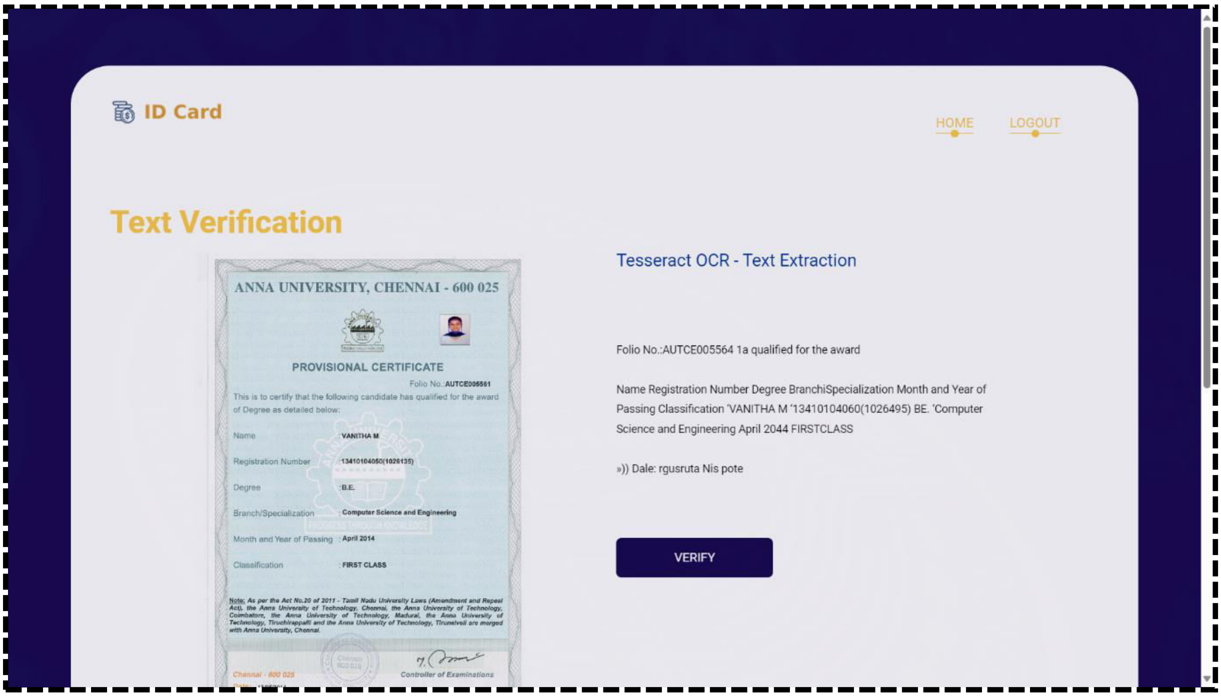
| DOI:10.15680/IJMRSET.2024.0707111 |





Name: DAYASHANKAR MISHRA
Date: 10/10/1994
PAN Card No.: CLUPM0440B

Information has matched..
Face has matched..
PAN Card is Genuine



ANNA UNIVERSITY, CHENNAI - 600 025

PROVISIONAL CERTIFICATE

Folio No.:AUTCE006561

This is to certify that the following candidate has qualified for the award of Degree as detailed below:

Name	:VANITHA M
Registration Number	:13410104050(1026135)
Degree	:B.E.
Branch/Specialization	:Computer Science and Engineering
Month and Year of Passing	:April 2014
Classification	:FIRST CLASS

Note: As per the Act No.20 of 2011 - Tamil Nadu University Laws (Amendment and Repeal Act), the Anna University of Technology, Chennai, the Anna University of Technology, Coimbatore, the Anna University of Technology, Madurai, the Anna University of Technology, Tiruchirappalli and the Anna University of Technology, Tirunelveli are merged with Anna University, Chennai.

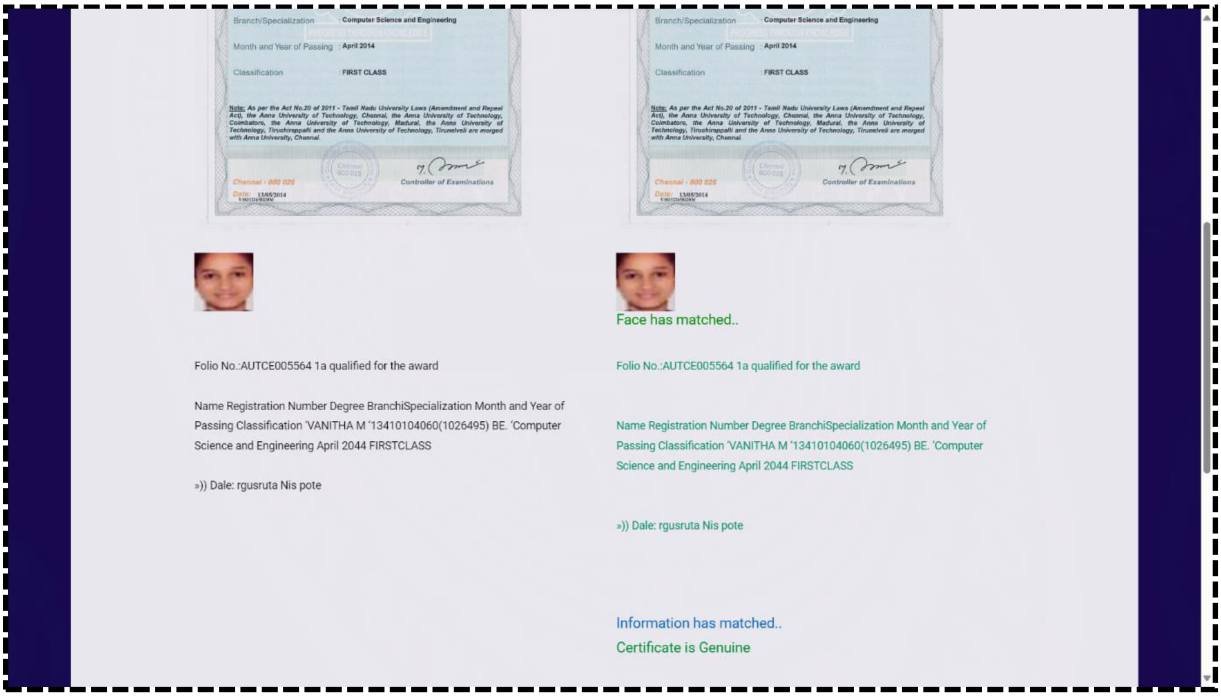
Chennai - 600 025 Controller of Examinations

Tesseract OCR - Text Extraction

Folio No.:AUTCE005564 1a qualified for the award

Name Registration Number Degree BranchiSpecialization Month and Year of Passing Classification 'VANITHA M '13410104060(1026495) BE. 'Computer Science and Engineering April 2044 FIRSTCLASS

»)) Dale: rgusruta Nis pote



Face has matched..

Folio No.:AUTCE005564 1a qualified for the award

Name Registration Number Degree BranchiSpecialization Month and Year of Passing Classification 'VANITHA M '13410104060(1026495) BE. 'Computer Science and Engineering April 2044 FIRSTCLASS

»)) Dale: rgusruta Nis pote

Information has matched..

Certificate is Genuine

VI. CONCULSION

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. Looking ahead, the project envisions deployment across diverse sectors, from access control to academic admissions and employment verification. The real-world validation of the system across various operational environments will solidify its performance and reliability. The project's impact extends beyond its technological achievements, contributing to a more secure and trustworthy document verification landscape in the digital era.

REFERENCES

1. R. Mudgalgundurao, P. Schuch, K. Raja, R. Ramachandra and N. Damer, "Pixel-wise supervision for presentation attack detection on identity document cards", IET Biometrics, vol. 11, no. 5, pp. 383-395, Sep. 2022.
2. T. Zichang et al., "Cross-batch hard example mining with pseudo large batch for ID vs. spot face recognition", IEEE Trans. Image Process., vol. 31, pp. 3224-3235, 2022.
3. M. Huber et al., "SYN-MAD 2022: Competition on face morphing attack detection based on privacy-aware synthetic training data", Proc. IEEE Int. Joint Conf. Biometrics (IJCB), pp. 1-10, Oct. 2022.
4. F. Boutros, N. Damer, F. Kirchbuchner and A. Kuijper, "Self-restrained triplet loss for accurate masked face recognition", Pattern Recognit., vol. 124, Apr. 2022.
5. Z. Zhu et al., "WebFace260m: A benchmark unveiling the power of million-scale deep face recognition", Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit., pp. 10492-10502, 2021.
6. R. Lara, A. Valenzuela, D. Schulz, J. Tapia and C. Busch, "Towards an efficient semantic segmentation method of ID cards for verification systems", arXiv:2111.12764, 2021.
7. 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.
8. Y. Viazovetskyi, V. Ivashkin and E. Kashin, "StyleGAN2 distillation for feed-forward image manipulation", Proc. Eur. Conf. Comput. Vis., pp. 170-186, 2020.
9. T. Karras, M. Aittala, J. Hellsten, S. Laine, J. Lehtinen and T. Aila, "Training generative adversarial networks with limited data", Proc. Adv. Neural Inf. Process. Syst., vol. 33, pp. 12104-12114, 2020.
10. V. Albiero et al., "Identity document to selfie face matching across adolescence", Proc. IEEE Int. Joint Conf. Biometrics (IJCB), pp. 1-9, Sep. 2020.

INTERNATIONAL JOURNAL OF
MULTIDISCIPLINARY RESEARCH
IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com