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

Nandhini V T [1], Sujitha R [2], Shruthi S [3]

Bachelor of Engineering, Electronics and Communication Engineering, Bannari Amman Institute of Technology, Erode, India

Bachelor of Engineering, Electronics and communication Engineering, Bannari Amman Institute of Technology, Erode, India

Bachelor of Engineering, Information Science and Engineering, Bannari Amman Institute of Technology, Erode, India

ABSTRACT

ID cards are sanctioned documents issued by government authorities or institutions to corroborate a person's identity. Educational instruments are sanctioned documents awarded by educational institutions, similar as seminaries, sodalities, and universities, to individualities who have successfully completed a specific program of study. They generally include the existent's name, snap, date of birth, a unique identification number, the name of the institution, the degree or qualification earned, the date of completion, and occasionally fresh details like the program of study or academic honors. Both documents play important places in colorful aspects of an existent's life, including employment, education, and sanctioned identification. Donation attacks on ID cards and educational instruments encompass a range of deceptive tactics employed by individualities with vicious intent to undermine the authentication and confirmation processes associated with these documents. These attacks can have different objects, from gaining unauthorized access to secured areas to securing employment or admissions under false pretenses. In the case of ID cards, common donation attacks involve phony, counterfeiting ways, print negotiation, tampering, and indeed the rationale of having lost one's ID card. On the other hand, educational instrument donation attacks include exercising warrants from parchment manufactories, falsifying academic reiterations, renew fraud, and indeed compromising credential verification systems. In response to this challenge, advanced technologies like Artificial Intelligence (AI) and deep literacy have surfaced as important tools for enhancing ID card fraud discovery. In this design, we claw into the development of an AIbased system designed to descry fraudulent ID cards and educational instruments. using the capabilities of deep inimical networks and TesseractOCR.The system aims to counter a range of donation attacks, including Bona Fide, compound, publish, and Screen attacks, which have grown decreasingly sophisticated. The emulsion of deep inimical networks and OCR technology offers a robust defense against the ever- evolving donation attacks on ID cards and educational instruments, icing document verification processes maintain their integrity in the face of decreasingly complex security challenges.

Keywords: *Artificial Intelligence, Fraud detection, Tesseract OCR, Machine learning, ID cards, Government authorities, False pretenses*

1. INTRODUCTION

Many different kinds of identification, such as worker's ID cards, driver's licenses, and national identity (ID) cards, have been introduced; however, because of how easily they can be falsified and manipulated, they have not assisted in addressing the problems of insecurity, fraud, or other vices for which they were intended. The prevalence of counterfeit identity cards has increased, making identity documents authentication and

verification a pressing concern in light of the rise in identity theft cases. When people identify themselves, they are asserting their identity based on a range of distinct qualifications, such as name, residence, birthday, place of birth, education, and employment history, among other things. These assertions, however, do not, by themselves, validate identity; supporting documentation is needed to confirm the validity of the identification document and the information it contains, as well as the individual's identity. The current ID card's simplicity made it very simple to alter and print it recklessly without the need for additional authentication or confirmation methods. Similar measures were taken by the voter's card and driver's license, which lack an automatic central reference mechanism to verify the legitimacy of their holders. Nevertheless, an ID card may have the photo of someone else with a different name or address due to these authentication errors. Replacement photo Attack on official documents (initially false documents with an arbitrary photo) or on authentic documents changed with a non-genuine photo. In order to accomplish this, the identity card business uses a variety of security and verification techniques, such as holograms, ultraviolet ink, and microprint, in addition to more sophisticated features like tamperproof laminates. These elements confirm the legitimacy of the card itself, but they don't confirm the identification on the card. In order to accomplish this, the identity card would need to connect to a real-time central database that confirms the owner's eligibility to possess the card.

Any document that can be used to establish someone's identify is an identity document, sometimes known as an ID piece, papers, or simply a piece of identification.On the other hand, if issued in a compact typical credit card size form, it is commonly referred to as an identity card (IC).(a) While some nations use official identity documents, such as public identification cards, which may be required or optional, others may use informal or indigenous identification to verify identity. Print ID refers to an identity document that includes a person's photo. Many nations will accept a driver's license as proof of identity when there isn't a formal identity document. Many nations require all foreign nationals, including those without a residence permit, to always have a passport or, occasionally, a public identity card from their home country on hand. The identity document serves as a link between an individual and their personal data, often stored in a database. The individual and the document are linked by the print and possession of it. Specific information on the document, such as the deliverer's full name, age, birthdate, residence, identification number, card number, gender, citizenship, and more, forms the basis of the relationship between the identity document and information database. The most secure method is a unique public identification number, however several nations require comparable numbers or do not mention them.

2. PROPOSED SYSTEM

2.1 EXISTING SYSTEM

Presenting fictitious or altered identification cards or educational credentials in order to receive benefits, services, or access to restricted locations is a typical tactic used by identity fraudsters to carry out their crimes. Fraudsters might, for instance, use fictitious ID cards to apply for loans, create bank accounts, rent real estate, or travel internationally. In a similar vein, con artists might apply for jobs, scholarships, visas, or admittance to colleges or universities using falsified or changed academic credentials. Numerous techniques, including manual inspection, rule-based systems, and supervised learning, have been devised and implemented to identify and stop such fraudulent operations. But these techniques have a number of shortcomings and restrictions.

. To overcome these limitations and drawbacks, this paper proposes an AI-based system for fraud detection using deep adversarial networks and Tesseract OCR. Our system consists of four main components:

Deep Adversarial Network Architecture: The system features a sophisticated architecture incorporating specialized subnetworks dedicated to the detection of various presentation attacks, including Bona Fide, Composite, Print, and Screen attacks. Training techniques such as Generative Adversarial Networks (GANs) are implemented to facilitate adversarial competition and learning among these subnetworks.

Tesseract OCR Integration: Integration of Tesseract OCR stands as a vital element, enhancing the system's capability to efficiently extract and analyze textual information from documents. The OCR technology plays a pivotal role in validating the authenticity of textual content present in ID cards and certificates.

Anomaly Detection: The proposed system incorporates advanced algorithms for identifying anomalies and discrepancies in both visual and textual elements of ID cards and certificates. Leveraging the power of deep adversarial networks, the system excels in recognizing subtle alterations that may elude human perception. Tesseract OCR is utilized to validate textual information and further enhance anomaly detection.

Ensemble Learning: To ensure comprehensive document validation, the system employs ensemble learning techniques, combining outputs from subnetworks and OCR-based textual analysis.

2.2 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-backed integrity. 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.

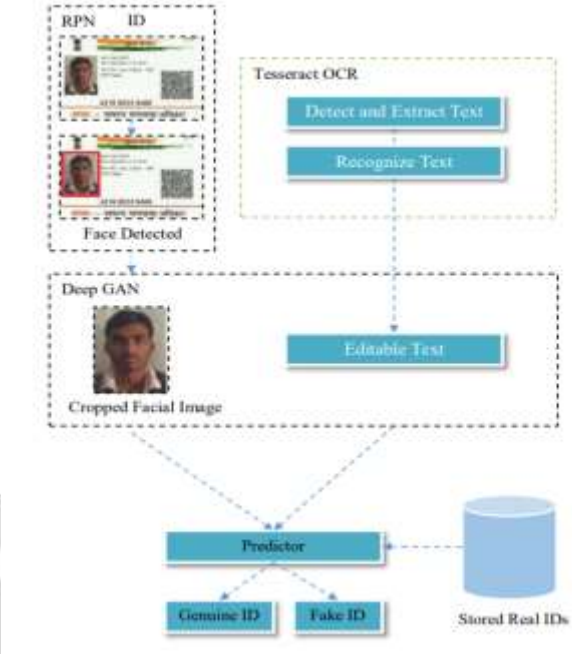

Figure 1. System Flow Diagram

2.3 DATABASE DESIGN

The database design for the id card fraud detection system comprises of various table which are as follows.

In the "Id Card Issuer" table, essential information about the issuers responsible for generating ID cards is stored. This includes fields such as "User name" and "Password" to authenticate and authorize the issuers accessing the system.

Table Name: Id Card Issuer					
S.no	**Field**	**Data type**	**Field size**	**Constraint**	**Description**
1	User name	Varchar	20	Null	Issuer name
2	Password	Varchar	20	Null	Issuer Password

Table 1. Id card Issuer

The "Generation" table records the generation of ID cards, linking them to specific cardholders through the "Cardholder Id" field. It includes an "Id" field for unique identification of each generation event, a "Decryption key" field for secure access to the generated ID cards, and a "Date time" field to timestamp when the generation occurred.

Table Name: Generation					
S.no	**Field**	**Data**	**Field size**	**Constraint**	**Description**

		type			
1	Id	Int	11	Null	Id
2	Cardholder Id	Varchar	20	Foreign key	Cardholder Id
3	Decryption key	Varchar	20	Null	Decryption key
4	Date time	Timestamp	Timestamp	Null	Date time

Table 2. Generation

The "Holder Details" table captures comprehensive details about the individuals holding the ID cards. This includes personal information such as name, gender, date of birth, address, contact details like mobile number and email, as well as unique identifiers like Aadhar number, PAN card number, and certificate number. The table also includes a link to the issued ID card and a unique "Cardholder Id" to identify each individual holder. Additionally, there's a "Password" field for authentication purposes and a "Register date" field to track when the holder details were registered in the system.

Table Name: Holder Details					
S.no	**Field**	**Data type**	**Field size**	**Constraint**	**Description**
1	Id	Int	11	Null	Id
2	Name	Varchar	20	Null	Name
3	Gender	Varchar	10	Null	Gender
4	Dob	Varchar	20	Null	Dob
5	Address	Varchar	50	Null	Address
6	Mobile number	Bigint	20	Null	Mobile number
7	Email	Varchar	30	Null	Email
8	Aadhar number	Varchar	20	Null	Aadhar number
9	Pancard Number	Varchar	20	Null	Pan card number
10	Certificate Number	Varchar	20	Null	Certificate number
11	Issued Id card link	Varchar	50	Null	Issued Id card link
12	Cardholder Id	Varchar	20	Primary key	Cardholder Id
13	Password	Varchar	30	Null	Password
14	Register date	Timestamp	Timestamp	Null	Register date

Table 3 . Holder Details

3. 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.

3.1 METHODOLOGY

The system flow of the AI-Based ID Card and Educational Certificate Fraud Detection System involves a series of interconnected modules and processes that collectively ensure a comprehensive and effective approach to document verification. Here's an overview of the system flow:

3.1.1 Fraud Detector Dashboard:

Users access the central interface for monitoring and managing the system and real-time insights into fraud detection metrics are provided through dynamic charts and graphs.

3.1.2 End User Control Panel:

The system involves three types of users: Generator-Certificate Issuer, Verifier-Certificate Verifier, and ID or Certificate Holder. The Generator inputs relevant details to generate and issue ID cards or certificates, using AI capabilities to ensure the integrity of generated documents. The Generator also maintains a secure and centralized database of issued credentials. The Verifier inputs or scans document details for verification, and fraud detection algorithms are triggered for accurate verification results. The ID or Certificate Holder presents their credentials for verification, and receives quick feedback on document authenticity.

3.1.3 Preprocessing Module:

Grayscale Conversion simplifies color information for standardized image format. Resize ensures uniformity in document image dimensions for efficient processing. Noise Filter reduces unwanted artifacts or

disturbances in document images. Binarization converts grayscale images into binary images for simplified representation.

3.1.4 Face Region Detector:

Utilizes Region Proposal Network (RPN) to identify and locate facial portraits within document images. RPN efficiently generates candidate regions likely to contain facial features, contributing to accurate facial recognition.

3.1.5 Attack Detector:

The system uses an Auto Encoder Module and an Auto Decoder Module to encode and decode document images into a latent space representation, learning essential features and establishing a baseline for normal variations. The system also has two phases: training and detection. In the training phase, the system learns the baseline, while in the detection phase, the system identifies and mitigates potential attacks on ID cards or certificates, using the outputs of the Auto Encoder and Auto Decoder. The system acts as a proactive defense mechanism against sophisticated attacks on documents.

The interconnected flow of these modules ensures a seamless and robust process for detecting fraudulent ID cards and educational certificates, covering various presentation attack scenarios. The system's effectiveness lies in the synergy of these components, offering a reliable solution for document verification.

3.2 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 with high 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 with the Verifier-Certificate Verifier module	System verifies the genuine document and provides positive feedback	Genuine document verified successfully	Pass

Table 4. Test Report

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.

4. 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. 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.

5. 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 millionscale 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 feedforward 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.

11.X. Wang, S. Wang, C. Chi, S. Zhang and T. Mei, "Loss function search for face recognition", Proc. ICML, pp. 10029-10038, 2020.

12.X. Zhu et al., "Large-scale bisample learning on ID versus spot face recognition", Int. J. Comput. Vis., vol. 127, no. 6, pp. 684-700, 2019.

13.Y. Shi and A. K. Jain, "DocFace+: ID document to selfie matching", IEEE Trans. Biometrics Behav. Identity Sci., vol. 1, no. 1, pp. 56-67, Jan. 2019.

14.J. Hernandez-Ortega, J. Galbally, J. Fiérrez, R. Haraksim and L. Beslay, "FaceQnet: Quality assessment for face recognition based on deep learning", Proc. Int. Conf. Biometrics (ICB), pp. 1-8, Jun. 2019.

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