Voter's Recognition and Fake Using Digital Image Processing and Deep Learning in Multiple Voters Real Time

Jeevan Sudheesh[1], Pranav P.G[2], Sreenandha Krishnan M.S[3], Mohammed Sinan[4], Viswajith C.K[5],Jayasoorya M.S[6],Ajith P.J[7],Bindu Anto[8]

[1] *Student, Computer Engineering, KKMMPTC Mala ,Kerala, India*
[2]*Student, Computer Engineering, KKMMPTC Mala ,Kerala, India*
[3] *Student, Computer Engineering, KKMMPTC Mala ,Kerala, India*
[4] *Student, Computer Engineering, KKMMPTC Mala ,Kerala, India*
[5]*Student, Computer Engineering, KKMMPTC Mala ,Kerala, India*
[6]*Student, Computer Engineering, KKMMPTC Mala ,Kerala, India*
[7]*HOD, Robotics Process Automation, KKMMPTC Mala ,Kerala, India*
[8]*HOD, Computer Engineering, KKMMPTC Mala ,Kerala, India*

ABSTRACT

The fundamental right to vote in elections is a cornerstone of democratic citizenship. In the modern era, Electronic Voting Machines (EVMs) have been introduced, marking a significant departure from the traditional voting system in India that used paper ballots and ballot boxes. Creating a secure voting system that maintains the privacy of conventional voting methods, ensures proper voter authentication, and promotes transparency has been a long-standing challenge. Previously, the use of paper ballots was time-consuming and susceptible to malpractices like booth-capturing and ballot-box stuffing, leading to disputes and delayed election results. In this project, we propose an EVM system that employs a deep Convolutional Neural Network (CNN)-based face recognition technology to capture a voter's facial image. This image is then verified against pre-captured images in the database. If the verification is successful, the system identifies the voter as valid and allows them to cast their vote for a political party. After voting, the voter's facial data is removed from the system, ensuring that each voter can only vote once. Face recognition is the process of identifying an individual from an image of their face by comparing it to a database of known faces. While this is a relatively straightforward task for most humans, "unconstrained" face recognition by machines, particularly in settings like malls, casinos, and transport terminals, remains an ongoing and active area of research. In recent years, the availability of a vast amount of photos crawled by search engines and uploaded to social networks, containing various unconstrained elements such as objects, faces, and scenes, has spurred advances in the field of image classification, facilitated by increased computational resources and more powerful statistical models.

Keyword *: -EVM-Electronic Voting Machine ,CCN-Convolutional Neural Network ,voter authentication,booth-capturing ,ballot-box stuffing,Face recognition etc…*

1. INTRODUCTION

The fundamental right to vote in elections is a cornerstone of democratic citizenship. In the modern era, Electronic Voting Machines (EVMs) have been introduced in India, replacing the traditional paper ballot and ballot box system. This shift aims to address issues like time-consuming processes and malpractices in elections, such as booth-capturing and ballot-box stuffing, which often led to disputes and delayed results. To ensure a secure and efficient voting system, this project proposes an EVM system that utilizes a deep Convolutional Neural Network (CNN)-based face recognition technology. This technology captures a voter's facial image, verifies it against a pre-captured database, and if successful, allows the voter to cast their vote. After voting, the voter's facial data is promptly removed from the system, preventing multiple votes from a single individual. Face recognition, a process of identifying individuals from facial images, is crucial in this context, and its application in "unconstrained" settings, like malls and transport terminals, is an active area of research driven by advancements in image classification and increased computational resources.

2. MILESTONES

In June 2020, a paper titled "Advanced Voting Machine Using Face Recognition," authored by A. Samundeeswari, P. Parthasarathy, C. K. Ragul, and K. Raguram, was published in Volume 8, Issue 6 of the International Journal of Computer Research and Technology (IJCRT) with the ISSN 2320-2882 [1]. Electoral fraud, also known as election fraud, constitutes an unlawful interference with the electoral process, involving voters casting repeated votes in favor of a specific party, thereby inflating their share of the vote. To ensure the ethical conduct of elections, it is imperative to eradicate such fraudulent practices. Consequently, a proposal has been put forth for an automated voting system leveraging Convolutional Neural Network (CNN) technology. Existing systems suffer from inefficiency due to their reliance on manual processes that are both time-consuming and challenging to maintain. Currently, various biometric methods are available, with face detection being the most efficient among them. The proposed system aims to create an automated voting process that operates without human intervention. This system incorporates a camera to capture electors' images, storing them in a database for subsequent analysis. Data analysis will be conducted on this database. In this approach, all labeled images undergo training through a convolutional neural network to predict and classify the images, achieving an accuracy rate of approximately 90%.

In 2008 ,This paper titled “R. Collobert and J. Weston, A unified architecture for natural language processing: Deep neural networks with multitask learning, Proc. 25th Int. Conf. Mach. Learn., pp. 160167,”[2].We present a single convolutional neural network architecture that, when given a sentence, produces various language processing predictions. These predictions encompass part-of-speech tags, sentence chunks, named entity tags, semantic roles, semantically related words, and an assessment of the sentence's grammatical and semantic coherence using a language model. This network is trained collectively on all these tasks through weight-sharing, which is a form of multitask learning. All tasks, except for the language model, utilize labeled data. The language model, on the other hand, learns from unlabeled text, showcasing a unique type of semi-supervised learning for these shared tasks. Our study demonstrates how both multitask learning and semi-supervised learning enhance the overall performance of these shared tasks, leading to state-of-the-art results

In 2019, E. Vetrimani and Dr. M. Arulselvi published a paper titled "Computerized Online Voting System using RFID Technology and Image Processing" in Volume 11, Issue 1 of the Singaporean Journal of Scientific Research (SJSR), which is part of the International Journal (AMIJ) [3].In this innovative approach, the system incorporates a two-step verification process. Initially, it validates voters through RFID data verification, followed by successful face authentication, granting them the privilege to cast their votes for their preferred candidate. These two novel authentication techniques in the voting system are designed to mitigate issues related to voter fraud and counterfeit votes.Currently, India employs two types of voting systems: the secret ballot paper and Electronic Voting Machines (EVMs). However, both of these methods have their limitations and drawbacks. India has yet to implement a computerized voting system. The existing voting systems are both insecure and time-consuming. They are susceptible to unauthorized voting, potentially leading to various issues.Hence, in this concept, we propose an effective voting system with two layers of security. The first layer involves verifying the RFID number, and the second layer employs face recognition. Our system significantly enhances security by implementing these new methods for each voter. User authentication is further bolstered by the incorporation of face recognition, which can determine whether a user is authorized or not.

In 2015,"M. Liang and X. Hu, Recurrent convolutional neural network for object recognition", 2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR). pp. 33673375, [4].In recent years, convolutional neural networks (CNNs) have achieved remarkable success in various computer vision tasks. Drawing some inspiration from neuroscience, CNNs share several characteristics with the brain's visual system. One notable difference is that while CNNs typically follow a feed-forward architecture, the visual system in the brain prominently features recurrent connections. Taking cues from this disparity, we introduce a recurrent CNN (RCNN) for object recognition by incorporating recurrent connections within each convolutional layer. Despite the input being static, RCNN units' activities evolve over time, allowing each unit's behavior to be influenced by its neighboring units. This characteristic enhances the model's capability to incorporate contextual information, a crucial aspect of object recognition. Similar to other recurrent neural networks, unfolding the RCNN over time results in a network of arbitrary depth with a fixed number of parameters. Additionally, the unfolded network encompasses multiple pathways, which can facilitate the learning process. We assess the model's performance on four standard object recognition datasets: CIFAR-10, CIFAR-100, MNIST, and SVHN. Remarkably, even with fewer trainable parameters, RCNN surpasses state-of-the-art models on all these datasets. Furthermore, increasing the number of parameters yields even better performance. These outcomes underscore the advantages of the recurrent structure compared to a purely feed-forward architecture for object recognition.

"Christian Szegedy, Wei Liu, Yangqing Jia, Pierre Sermanet, Scott Reed, Dragomir Anguelov, Dumitru Erhan, Vincent Vanhoucke,Andrew Rabi-novich: Going Deeper with Convolutions. Computer Vision and Pattern Recognition." [5].We introduce a deep convolutional neural network design known as Inception, which played a pivotal role in establishing a new state-of-the-art standard for classification and detection during the ImageNet Large-Scale Visual Recognition Challenge 2014 (ILSVRC14). The key distinguishing feature of this architecture lies in its superior utilization of computational resources within the network. This achievement was made possible through a meticulously crafted design strategy that allows for increasing both the depth and width of the network while maintaining a consistent computational budget. In pursuit of optimizing quality, our architectural decisions were guided by the Hebbian principle and the concept of multi-scale processing. One specific variant of this architecture, named GoogLeNet, was utilized in our ILSVRC14 submission. It boasts a depth of 22 layers and is assessed for its performance in the realms of classification and detection.

In 2004, Tadayoshi Kohno and colleagues conducted an analysis of an electronic voting system, presenting their findings at the IEEE Symposium on Security and Privacy in that same year [6]. Amidst the availability of substantial federal funds in the United States for the replacement of outdated punch-card and mechanical voting systems, many municipalities and states are transitioning to paperless electronic voting systems offered by various vendors. We have conducted a comprehensive security analysis of the source code of one such voting machine, which holds a significant market share. Our analysis has revealed that this particular voting system falls considerably short of even the most basic security standards applied in other domains.We have identified multiple issues, including unauthorized privilege escalation, improper use of cryptography, susceptibility to network-based threats, and subpar software development practices. Our findings indicate that voters, without any internal access privileges, can cast an unlimited number of votes without detection by the voting terminal software's mechanisms. Additionally, we have demonstrated that even the most severe external attacks could have been executed without requiring access to the source code. In light of these vulnerabilities, concerns about insider threats are not the sole worry; external actors can also exploit these weaknesses. Furthermore, we have shown that insider threats, such as poll workers, can not only manipulate votes but also compromise voter privacy by matching votes to individual voters. As a result, we conclude that this particular voting system is unsuitable for use in a general election. It is possible that other paperless electronic voting systems may suffer from similar flaws, regardless of any certifications they may have received. Therefore, we recommend the adoption of voting systems with a voter-verifiable audit trail, where a computerized voting system generates a paper ballot that can be reviewed and confirmed by the voter.

In 2020.A "Smart Voting System" by CH CHANDRA MOULI is accessible through SSRN under reference number 3690115, and it was made available in [7]. This paper introduces an innovative certification method for online voting systems, which relies on facial detection of the voter. In India, there are currently two prevailing voting methods in practice: the secret ballot paper and Electronic Voting Machines (EVMs). However, both of these methods come with certain limitations. Implementing online voting in India poses a unique challenge.The existing

voting system lacks robust security measures, requiring voters to travel to polling booths and endure long queues to cast their votes. This often results in missed opportunities to vote. Additionally, individuals who are not eligible to vote may do so through fraudulent means, leading to various issues. Therefore, this paper proposes an exceptionally efficient voting system.In this proposed system, we incorporate three layers of security in the voting process. The first level involves authenticating the Aadhar number, the second level authenticates the Voter ID, and the third level employs facial matching. The security of our system is significantly enhanced through the application of this novel approach for each voter. Furthermore, the user authentication process is strengthened by the inclusion of face detection within the application, which verifies whether the user is indeed an authenticated voter.

published in 2020. In the "International Journal of Innovative Research in Technology", Priyadarshini and her co-authors presented their work on the design and implementation of an RFID-based smart voting system incorporating frontal face recognition techniques, as detailed in their paper spanning pages 338 to 343 [8]. The fundamental pillar of a nation's democracy lies in the act of voting, through which citizens select their preferred candidate to lead the nation. The infiltration of unlawful practices can jeopardize the integrity of this process and place the nation's governance in the wrong hands. Governments employ various methods to prevent electoral malpractices, but one area that still lacks comprehensive security is the voter verification process. Currently, this process is manual in many countries, demanding a significant workforce.This paper primarily addresses the challenges and potential crimes associated with the voter verification process. The proposed system collects and stores voter details, fingerprints, and facial data in a database beforehand. Each voter is issued an RFID card, serving as their voter ID and containing personal information. On the day of voting, the voter undergoes a meticulous three-level verification process.Firstly, the RFID card is scanned by an RFID reader, displaying the individual's information on an LCD screen. Subsequently, the voter is required to confirm their identity by verifying their fingerprint. The fingerprint reader checks the provided fingerprint against the database. If all the details align in this initial phase, the process proceeds to the next level. Here, the system recognizes the voter's face and compares it to the existing database. Only when all three verification levels are successfully matched does the ballot booth door open, permitting the voter to cast their vote. If any of the verifications fail, the voter is denied the opportunity to vote.Furthermore, the paper emphasizes that the election results are simultaneously displayed on a monitor. This secured verification process effectively combats proxy voting, political party interference, and other illicit activities during Election Day, ensuring the integrity of the electoral process.

A paper by the name "Smart Voting System Through Face Recognition" was published by Kumar, Aman and Vishwash Kumar[9]. In this paper, a novel authentication method for online voting systems using facial recognition ofthe voter is introduced. In India, there are currently two prevailing voting methods: the secret ballot paper and Electronic Voting Machines (EVMs). However, both of these processes come with certain limitations. Importantly, online voting has not yet been implemented in India. The existing voting system is also not entirely secure.Under the current system, voters are required to visit various polling booths and endure long queues to cast their votes, resulting in missed opportunities for many citizens. Additionally, individuals who are ineligible may cast their votes fraudulently, leading to numerous issues. Therefore, this project aims to propose an efficient and effective voting system. In our approach, we implement a three-tier security system in the voting process. The first level involves the verification of a unique identification number (UID), the second level verifies the election identification number (EID), and the third level employs facial recognition or face matching. This new application method significantly enhances the security level of our system for each voter. Furthermore, the user authentication process is bolstered by the incorporation of face recognition into the application, which determines whether a specific user is an authenticated voter or not.

In 2017 .“E. Shelhamer, J. Long, and T. Darrell, Fully Convolutional Networks for Semantic Segmentation”, IEEE Trans. Pattern Anal. Mach. Intell.. vol. 39, no. 4, pp. 640651, .[10]. Convolutional networks are potent visual models that generate hierarchies of features. We demonstrate that when convolutional networks are trained end-to-end, handling input from pixels to pixels, they surpass previous best results in semantic segmentation. Our innovative approach involves constructing "fully convolutional" networks capable of processing inputs of various sizes and producing correspondingly-sized outputs efficiently during both inference and learning. We define and elaborate on the concept of fully convolutional networks, elucidating their suitability for tasks requiring dense spatial prediction, and establishing connections to prior models. We transform contemporary classification networks like AlexNet, the VGG net, and GoogLeNet into fully convolutional networks and adapt their learned representations through fine-

tuning for segmentation tasks. Furthermore, we introduce a skip architecture that combines semantic information from a deep, coarse layer with appearance details from a shallow, fine layer, resulting in precise and detailed segmentations. Our fully convolutional networks achieve enhanced segmentation performance on datasets like PASCAL VOC (a 30% relative improvement, reaching a mean IU of 67.2% in 2012), NYUDv2, SIFT Flow, and PASCAL-Context. Remarkably, the inference time for a typical image is reduced to one-tenth of a second.

"Y. LeCun, Backpropagation Applied to Handwritten Zip Code Recog- nition, Neural Comput.", vol. 1, no. 4, pp. 541551, Dec. 1989 [11]. This paper showcases the significant improvement in the generalization ability of learning networks when task-specific constraints are incorporated. The method demonstrated here integrates these constraints into a backpropagation network by shaping the network's architecture. This technique has proven effective in recognizing handwritten zip code digits as provided by the U.S. Postal Service. In this process, a single network is capable of learning the complete recognition process, starting from the normalized character image and concluding with the final classification.

In 2015,"Florian Schroff, Dmitry Kalenichenko, James Philbin.": FaceNet: A Uni- fied Embedding for Face Recognition and Clustering Proceedings of the IEEE.[12]. Despite recent advancements in face recognition techniques [10, 14, 15, 17], efficiently implementing face verification and recognition at scale remains a significant challenge for existing methods. In this paper, we introduce FaceNet, a system that directly learns to map face images into a condensed Euclidean space, where distances directly represent facial similarity. Once this space is generated, tasks like face recognition, verification, and clustering can be easily performed using FaceNet embeddings as feature vectors. Unlike previous deep learning approaches, our method utilizes a deep convolutional network that optimizes the embedding itself rather than relying on an intermediate bottleneck layer. For training, we employ triplets of approximately aligned matching and non-matching face patches, generated through an innovative online triplet mining approach. The key advantage of our approach is its exceptional representational efficiency, achieving state-of-the-art face recognition performance while requiring only 128 bytes per face. On the widely recognized Labeled Faces in the Wild (LFW) dataset, our system attains a remarkable new accuracy record of 99.63%. Similarly, on the YouTube Faces DB, it achieves an accuracy of 95.12%. In comparison to the best published results [15], our system reduces the error rate by 30% on both datasets.

3.CONCLUSIONS

Face recognition presents numerous challenges in the realm of visual analysis. Identifying human faces is a complex task due to the wide range of variables, including age, expressions, facial features like nose shape, and the distance between eyes. Consequently, this technology holds significant importance in security applications, such as verifying legal documents and identifying potential threats in public spaces like railway stations, ports, and shopping malls. Despite various techniques demonstrating effectiveness in detecting and recognizing human faces, developing a computationally efficient algorithm for matching human faces with a large database remains a challenging endeavor. Face recognition can be considered a sophisticated computer vision task, and machine learning models like Support Vector Machines (SVM), random forests, and powerful classifiers such as artificial neural networks have shown promise in achieving reasonable performance in this field.

In this paper, we introduce a secure and user-friendly electronic voting machine that relies on face recognition. The primary aim is to address issues related to tampering and security during elections in India. Our proposed method has been tested in real-time scenarios and performs well on standard benchmark datasets as well as a custom dataset we created. The improved performance can be attributed to the deep architecture of convolutional neural networks (CNNs).

Over the past two decades, various government-owned companies in India have conducted elections using electronic voting machines (EVMs), simplifying the voting process and enhancing reliability. However, recent reports of irregular usage have emerged. Our method offers a standalone authentication system that could augment the existing EVMs, aligning with business and customer satisfaction objectives.

4. REFERENCES

[1] A Samundeeswari , P Parthasarathy,C K Ragul,K Raguram, Advanced Voting Machine Using Face Recognition, 2020 IJCRT Volume 8, Issue 6 June 2020 ISSN: 2320-2882
[2]R. Collobert and J. Weston, A unified architecture for natural language processing: Deep neural networks with multitask learning, Proc. 25th Int. Conf. Mach. Learn., pp. 160167, 2008
[3] E.Vetrimani AND Dr.M.Arulselvi, Computerized Online Voting System using RFID Technology and Image Processing, An International Journal (AMIJ) Singaporean Journal of Scientific Research(SJSR) Vol.11.No.1 2019.
[4] M. Liang and X. Hu, Recurrent convolutional neural network for object recognition, 2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR). pp. 33673375, 2015.
[5] Christian Szegedy, Wei Liu, Yangqing Jia, Pierre Sermanet, Scott Reed, Dragomir Anguelov, Dumitru Erhan, Vincent Vanhoucke,Andrew Rabi-novich: Going Deeper with Convolutions. Computer Vision and Pattern Recognition.
[6] Kohno, Tadayoshi, et al. Analysis of an electronic voting system. IEEE Symposium on Security and Privacy, 2004. Proceedings. 2004. IEEE, 2004.
[7] MOULI, CH CHANDRA. Smart Voting System. Available at SSRN 3690115 (2020).
[8] Priyadarshini, Mrs R., et al. Design and realization of RFID based smart voting system with frontal face recognition technique. International journal of innovative research in technology 6.12 (2020): 338-343.
[9] Kumar, Aman, and Vishwash Kumar, "Smart Voting System Through Face Recognition".
[10] E. Shelhamer, J. Long, and T. Darrell, Fully Convolutional Networks for Semantic Segmentation, IEEE Trans. Pattern Anal. Mach. Intell.. vol. 39, no. 4, pp. 640651, 2017.
[11] Y. LeCun, Backpropagation Applied to Handwritten Zip Code Recog- nition, Neural Comput., vol. 1, no. 4, pp. 541551, Dec. 1989
[12] Florian Schroff, Dmitry Kalenichenko, James Philbin.: FaceNet: A Uni- fied Embedding for Face Recognition and Clustering Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition 2015. Publisher, Boston, MA (2015)