International Journal of Scientific Research in Science and Technology
Print ISSN: 2395-6011 | Online ISSN: 2395-602X (www.ijsrst.com)
doi : https://doi.org/10.32628/IJSRST218318

A Survey on Performing E-Voting through Facial Recognition

Pratik Hopal, Alkesh Kothar, Swamini Pimpale, Pratiksha More, Jaydeep Patil
Information Technology Department, AISSMS Institute of Information Technology, Pune, Maharashtra, India

Article Info
Volume 8, Issue 3
Page Number : 141-147

Publication Issue
May-June-2021

Article History
Accepted : 07 May 2021
Published : 14 May 2021

ABSTRACT

The election procedure is one of the most essential processes to take place in a democracy. Even though there have been immense technological advancements, the process of election has been highly limited. Most of the election procedures have been performed using ballot boxes which is an old process and needs to be updated. The security of such practices is also a concern as the identification of the voters is being done manually by the election officers. This process also needs an improvement to increase accuracy and reduce human errors by automating the process. Therefore, for this purpose, this research article analyzes the previous researches on this paradigm. This allows an effective understanding of the machine learning algorithms that are used for automatic facial recognition in the E-voting systems. This paper comes to the conclusion that the Recurrent Neural Networks are best suited for such an application for facial recognition. The future editions of this research will elaborate more on the proposed system in detail.

Keywords : Facial feautures, E-Voting, Recurrent Neural networks.

I. INTRODUCTION

Elections are an essential procedure that is performed to enact and maintain the democracy of a particular nation. Elections decide the administrative head of the country by taking into consideration the opinions of every citizen of the country. This process is known as an election, wherein the interested candidates are allotted by the political parties, and the citizen's vote for the interested candidates. This process is highly necessary to enable the effective leadership of the country.

Elections are a construct of the democracy where the government is by the people and for the people. This was not the case earlier wherein monarchy was highly popular and widely followed leadership in a particular area. This type of government has a king as a leader and the administrative and judicial head of the country. The king is assisted by his ministers in various internal as well as external affairs of the country. The leadership is transferred through the bloodline, where the king's son becomes the heir to the throne.

Even though this type of governance model was highly popular and widely used, it eventually got replaced by democracies all over the world. This is due to the inherent flaws in the governance model that was noticed eventually. There are still some monarchies that are functioning around the world, but they are a minority in comparison with democratic countries.

The democracies are highly fair in their execution and are a preferred model for governance in the majority of the world currently. Democracy allows the citizens of the country to elect their representative to be the administrative head of the country. Democracy enables a much more transparent and satisfactory form of governance which involves the people of the country at a grassroots level which is extremely necessary.

The election is the procedure that is performed in this regard. The election procedure is a lengthy process by which, certain political parties announce their candidates. These candidates contest the election by filling up the requisite formalities. The election commission is in charge of the election procedure and is immune to a significant amount of intervention by the political or government agencies. This is an independent organization that facilitates the entire election procedure effectively and with transparency.

In the process of facilitating the effective implementation of security in the election procedure, there can be highly prominent features used, such as facial recognition. The process of facial recognition is highly effective in combating various attackers that disguise themselves to achieve malicious voting. There are several techniques to implement facial recognition automatically, out of which the most commonly used approaches are Data Mining and Image processing

Several Data mining approaches are identified for facial recognition such as MAFIA or Maximal Frequent Itemset Algorithm. MAFIA incorporates the use of non-edge and Edge images to mine the negative and positive feature patterns. The sliding window is utilized in the detection phases to effectively identify the individual in various expressions and orientations using the data mining approach.

Several more prominent techniques utilize the data mining approach to achieve effective facial recognition. But there are certain inconsistencies with the data mining approach, such as high space complexities that make it not suitable for an application in such constrained approaches.

Image processing techniques are also applicable to effectively identifying individuals through facial recognition automatically. Recurrent Neural Networks is an effective deep learning algorithm that are effectively utilized for facial recognition purposes. The RNN approach is highly flexible and is mostly utilized for enabling an effective realization of a memory control between layers of a neural network. But the image processing approaches also suffer from increased computational complexities that cannot be resolved effectively for implementation in a facial recognition approach.

Therefore, to implement facial recognition the paradigm of machine learning has been explored in this research paper. The machine learning approaches are effective in combatting the problems faced by the other approaches, namely Data mining.

An effective machine learning algorithm from the neural network family called Recurrent Neural Network is chosen for facial recognition. The RNN allows the effective implementation of the machine learning approach for facial recognition effectively. The RNN also overcomes the limitations posed by Data Mining as well as the Image processing approaches to achieve significant improvements.

This research paper dedicates section 2 for analysis of past work as literature survey, section 3 concludes the paper in detail.

II. LITERATURE SURVEY

Zuyina Ayuning Saputri presents the e-voting security system for anonymity voter authentication by using the technique of 1024-bit Shamir's algorithm. The architecture of the system consists of architecture on the client and server-side [1]. The preparation on the client-side involves the development of e-voting applications based on android. On the server-side, the architecture includes web architecture for recording and monitoring the location of voters as well as the web for recapitulation of voice count operations. The framework for e-voting that will be rendered is fitted with a security system to keep the authenticity of voting data by implementing Shamir's algorithm and SHA-1 algorithm. The architecture of the system depends on the specifications of the e-voting technique for the election of EEPIS BEM President.

Nazmul Islam [2] introduces new online voting (e-voting) scheme that uses confirmation numbers (CNs) and updated numbers simplified verifiable mixnet re-encryption (R-SVRM). CNs are special and publicly registered numbers that are revealed in their encrypted form. They are allocated to voters individually to make votes verifiable. Also, the operation and validation of cryptographic operations are easier than with CNS and R-SVRM based schemes. Besides, voters do not need to have their private keys to work with the authorities when encrypting votes. Again, R-SVRM is verifiable so, authorities do not need to sign a pair for each encrypted vote. Besides, a courageous individual cannot launch an attack due to disagreements between all votes and CN-related voting officers.

Oke B. A proposed technique that combined with the application of secure authentication algorithms in smart cards and fingerprint biometrics enables reliable MFA technology. All voters require a smart card and their fingerprints to vote. Each voter's data is encrypted using the developed Feistel block cipher and then stored on their respective smart cards [3]. Voter fingerprint samples are magnified using a first-moment feature extraction algorithm. The MFA method uses more than one credential to authenticate users. Several factors were taken into account when selecting the attachment of credentials for the authentication process. These include acceptance for the user, time for voter authentication, memory requirements for selected credentials.

Xin Jin introduces for face alignment, a new local half-voting-based technique. Using the spatial limitations imposed by the stationary facial components, the key concept of this approach is to direct the search for other facial points. This can be applied by first using nonparametric kernel smoothing to construct a voting map and then using multi-output ridge reression to combine it with a conventional response map. Their technique is depend on Constrained Local Models but is augmented with local Hough voting based technique to enhance the results. This local Hough voting technique is closely similar to the implicit shape model system (ISM) in which votes for the position of the object of interest were found by each local segment. In object recognition, ISM has made huge strides. However, it has not been used to smooth the forehead. The authors combine the local voting map and the answer map from the local detectors using the multi-output instead of searching specifically for the position with the most votes in the voting space. The proposed approach is reliable and easy to implement compared to other approaches[4].

Neel Ramakant Borkar [5] proposed a powerful PCA and LDA-based facial recognition system. The presented technique has 97 percent precision using the Raspberry Pi 3 module by combining these two hybrid techniques. The face is multidimensional and therefore has a “curse of dimensionality”. The face needs a lot of memory and time to process. To solve this problem, it is necessary to achieve the best features to improve accuracy and eliminate image noise. PCA is often used to reduce parameters. After the dimensions are reduced, the images are presented on eigenspace using LDA. The algorithms of PCA and LDA project all the images in the dataset of AT&T training into your own space. There are also unknown images, or test images, projected into one's own space. The Euclidean distance between the test image and all the training images is measured for identification. The proper match is the trained image with the smallest Euclidean distance to the test image, the unknown image.

Abdallah Meraoumia introduces a framework of a secure e-voting system for uses in an election. To recognize their identity, the proposed framework uses cryptographic techniques to ensure the security of voter information and multifaceted display technology. In the presented method, the display of the voter is centered on a card containing their zip code and biometric characteristics[6]. The authors use the fuzzy commitment scheme due to their strong robustness against cyber-attacks to develop a biometric cryptosystem to secure the operation of the election. Because of their promising findings, the authors choose PLV and PLP modalities. Moreover, an effective method based on the Gabor 2D philter for the extraction of feature vectors was used. The voter's data was encrypted with a random key to implementing the crypto limit. This key is then inserted using the fuzzy compromise theory into the voters' vector of characteristics (extracted from PLV and / or PLP). The terminal device transmits voter information during transmission in the form of an encrypted opinion (selected candidate), a fixed face (sample and key combination), and a key signature. Upon receipt, by introducing a new key extraction scheme, changing the function vector of the voter, matching this vector to the voter database, and finally enabling the voter to perform this procedure, the election centralized system removes the key from the set aspect and confirms accomplishment.

Irham Mulkan Rodiana [7] introduces e-poll architecture using public key infrastructure (PKI) and hash feature. The ease of implementation in the real world was later taken into account in this design, but the anonymous and validation aspects of the e-voting method were not removed. The proposed system consists of 5 phases, named as the registration phase, the voting phase, the end of the day phase, the central compilation phase, and the final phase of the deposit. The registration phase generates keys held by the voters, the voting stage is the stage that will be passed by the voters as the election takes place, in the end of the day phase the data from each selected ballot will be collected, in the central compilation phase each data set from the previous stage will be locked by a central committee public key and in the final phase of the deposit, verification becomes more difficult with an additional key from the central committee. The design proposed is acceptable for countries such as Indonesia that are wide and dispersed.

Aanjana Devi. S proposed a framework of an e-voting system that needs to be detected and recognized face using biometrics. For facial recognition and identification, the device uses two algorithms, such as viola Jones and the eigenface algorithm. To capture a personal face using a website or camera, the authors use the viola Jones algorithm and save it with voter information. Voters sit in front of a laptop or computer's camera connected to the voting server via a webcam or the internet at the time of voting, so the face is recorded and identified using the eigenface and the face in the database. A face image that matches is processed if it matches a face in the database the voters can notify candidates they want to vote for. Otherwise, voters will not be able to elect a leader by voting. [8].

Mohamed Nassar introduces a new safe and verifiable voting protocol[9]. The presented framework is composed of three parties. The first authority is the counting server, which is responsible for counting and transmitting encrypted results to the verifier. For any authentication failure, the counting server is responsible. As a consequence, it is strongly recommended that counting servers record fraudulent or double-voting voters and ignore those votes. The trustee or verifier server has to check the credibility of the results and there was no fraud on the part of the tallying server or the voters. Voters are authorized and authorized persons who cast their ballots in electoral terms (e.g., the number of votes allowed and the number of selections selected for a particular application). A client application helps the voters securely connecting to the two authorities and casting their votes.

Alfonso Brolin Sihite [10] presents an e-voting review and validation system that is likely to solve the problem of ballot voting. The e-voting system is equipped with an e-recap system that has the function of evaluating the ballots so that the results of this e-voting system can be seen, reviewed, and monitored by anyone. For the intent of who the voter is and is not specified in the recap outcomes, this e-voting and e-recap technique uses cryptographic hash function message authentication codes (MAC) and public key infrastructure (PKI). The polls are conducted so that they obey in the election the hidden rules, but it is possible to collect and analyze all the votes. Voters should review the ballots themselves so that when the e-recap system is applied, there is no difference in the votes. Elections should also be open, accountable, and subject to public scrutiny. With this e-voting and e-recap verification and validation method, which uses the application of MAC (cryptographic hash function message authentication codes) and public key infrastructure (PKI), it is expected that traditional elections will be replaced by e-voting.

Teguh Nurhadi Suharsono introduces the concept of metrics for measuring verification in an electronic voting system, where items are first determined and tested against the verification requirements of the electronic voting system. The degree of verification is obtained based on the value of the degree of anonymity which was previously calculated. Measurements are performed on a variety of evocation protocols that have been defined. By measuring the verification aspects of some electronic voting protocols, it is hoped that the verification can be measured on the protocol of the voting system [11].

L.Vetrivendan [12] presents a new authentication technology that has three levels of security to identify false voters. To distinguish false voters, the facial authentication technique is very useful to prevent false votes during an electoral commission. By signing into the presented smart internet voting system, voters can vote from anywhere. This is a one-time investment for the government as any transaction is done through an internet connection. It is not necessary to locate a voter, but their vote is necessary. Because the data is stored in a centralized repository, the data is available at any time and is stored in a central repository and possible to back up the data. Every minute, an intelligent voting system offers an updated outcome. Less manpower and resources are also needed. The database should be updated every year on or before an election so that new eligible citizens can be registered and those who have died are removed from the voter's list.

III. CONCLUSION

This research article deals with the shortcomings of the current scenario of the election procedure. The current election procedure is highly outdated and contains extensive loopholes. These create security concerns over the security of the election process. Therefore, this research identifies that there is a need for an effective facial recognition approach combined with the Electronic Voting system. This would allow an effective increase in the security and transparency of the whole election process. For this purpose, this survey paper has analyzed the related works in detail for their improvements and limitations. This has allowed the effective formulation of the e-voting approach through facial recognition using the Recurrent Neural Networks. The methodology will be discussed in the utmost detail in the upcoming editions of this research.

IV. REFERENCES

[1]. Zuyina Ayuning Saputri, Amang Sudarsono, Mike Yuliana, " E-voting security system for the election of EEPIS BEM president", International Electronics Symposium on Knowledge Creation and Intelligent Computing, 21 December 2017.

[2]. Nazmul Islam, Kazi Md. Rokibul Alam, Shinsuke Tamura, Yasuhiko Morimoto, “A new e-voting scheme based on revised simplified verifiable re-encryption mixnet”, 2017 International Conference on Networking, Systems and Security (NSysS), 27 March 2017.

[3]. B. A. Oke, O. M. Olaniyi, A. A. Aboaba, O. T. Arulogun, “Developing multifactor authentication technique for secure electronic voting system”, 2017 International Conference on Computing Networking and Informatics (ICCNI), 01 December 2017.

[4]. Xin Jin, Xiaoyang Tan Liang Zhou, “Face Alignment Using Local Hough Voting”, 2013 10th IEEE International Conference and Workshops on Automatic Face and Gesture Recognition (FG), 15 July 2013.

[5]. Neel Ramakant Borkar, Sonia Kuwelkar, “Real-time Implementation of Face Recognition System 2017 International Conference on Computing Methodologies and Communication (ICCMC), 8 February 2018.

[6]. Abdallah Meraoumia, Hakim Bendjenna, Mohamed Amroune, and Yahia Dris, “Towards a Secure Online E-voting Protocol Based on Palmprint Features”, 2018 3rd International Conference on Pattern Analysis and Intelligent Systems (PAIS), 03 January 2019.

[7]. Irham Mulkan Rodiana, Budi Rahardjo, Aciek Ida W, “Short Design of a Public Key Infrastructure-based Single Ballot E-Voting System”, 2018 International Conference on Information Technology Systems and Innovation (ICITSI), October 2018.

[8]. Aanjana Devi.S, Dr.Palanisamy.V and Anandha Jothi.R, “Confidential E-Voting System Using Face Detection and Recognition”, International Journal of Engineering and Techniques - Volume 3 Issue 4, July-Aug 2017.

[9]. Mohamed Nassar, Qutaibah Malluhi and Tanveer Khan, “A Scheme for Three-way Secure and Verifiable E-Voting”, 2018 IEEE/ACS 15th International Conference on Computer Systems and Applications (AICCSA), 17 January 2019.

[10]. Alfonso Brolin Sihite and Muhammad Salman, “E-Voting and e-Recap Verification and Validation Schemes for Indonesia Utilizing Cryptographic Hash Function Message Authentication Codes (MAC) and Public Key Infrastructure (PKI) ”, 2019 International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS), Oct 2019.

[11]. Teguh Nurhadi Suharsono, Kuspriyanto Kuspriyanto, and Budi Rahardjo, “Verifiability Metric Notion in e-Voting System”, 2019 IEEE

13th International Conference on Telecommunication Systems, Services, and Applications (TSSA), October 2019.

[12]. L.Vetrivendan, Dr.R.Viswanathan, and J.AngelinBlessy, “Smart Voting System Support through Face Recognition International Journal of Engineering Research in Computer Science and Engineering (IJERCSE), 4 April 2018.

Cite this article as :

Pratik Hopal, Alkesh Kothar, Swamini Pimpale, Pratiksha More, Jaydeep Patil, "A Survey on Performing E-Voting through Facial Recognition", International Journal of Scientific Research in Science and Technology (IJSRST), Online ISSN : 2395-602X, Print ISSN : 2395-6011, Volume 8 Issue 3, pp. 141-147, May-June 2021. Available at
doi : https://doi.org/10.32628/IJSRST218318
Journal URL : https://ijsrst.com/IJSRST218318