International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048
Volume 7, Issue 8, pp 141-147, August-2023
https://doi.org/10.47001/IRJIET/2023.708018

Parametric-Based Facial Recognition Technique for Improved Electronic Voting System

[1]Udochukwu Okeahialam, [2]Anthony I. Otuonye, [3]Mathew E. Nwanga

[1,2,3]Department of Information Technology, Federal University of Technology, Owerri, Nigeria
Authors E-mail: [1]udowilson2010@gmail.com, [2]anthony.otuonye@futo.edu.ng, [3]mathew.nwanga@futo.edu.ng

Abstract **- Voting process plays a key role in the national development, with the attendant cost of time and other resources in the election. Recently electronic voting is gaining ground in some African countries with full benefit of accuracy and data reliability. The work proposed a biometric facial recognition strategy driven with tokenized unique parameter authentication techniques for electronic voting that reduce time, expenses, and human effort. This system is more secure as it uses the mechanism of a multifactor authentication verification process implemented using a unique token sent through SMS. Results generated from the proposed system offered very precise and improve accuracy and performance. Election reliability is enhanced, confidentiality, time and cost effectiveness are achieved. Further result gotten from the system deployment shows that 40% and 32.6% of the respondents asserted strongly and strong respectively, that the new system can perform life face detection. In addition, 56% of the stakeholders considered accepted that the new system can work effectively with unique token in less than 5 minutes.**

Keywords: Face Recognition, Electronic Voting, Tokenized, Parametric Authentication, Election Reliability.

I. INTRODUCTION

Globally, election management has posed a plethora of challenges ranging from time and cost intake to errors and result manipulations. In most African countries like Nigeria, elections conducted are plagued with issues of voter disenfranchisement and voter apathy orchestrated by irregularities during election accreditation exercises. According to Mamokhere and Mabeba (2022), the credibility of the electoral process is an important factor to achieving a free, fair, transparent and comprehensible election to voters for an unbiased and uncompromised democratic transition.

The need to promote transparency, verifiability, accountability and overall reliability with minimal time and cost electioneering process has become a key ingredients for national development(Nguyen, Delahaies, Retraint, & Morain-Nicolier, 2019)(Panizo Alonso et al., 2021).The spate of election held in recent times has been characterized by inaccuracy of results and loss of confidence on the side of voters as a result of long computational time (Vignesh, Sricharan, Shankrith Chokkalingam, Bhuvana, & Bharathi, 2022). The long existence queuing witnessed in the process made the majority of the individuals to pass up on the opportunity of casting their votes. In addition, individuals who are not qualified to cast their votes, usually find undesirable methods to do so, which may cause diverse issues in electioneering management and may amount to inaccurate results with huge negative marks(Venkata and Bhaskarrao 2020).

Current pervasiveness of digitalization in every aspect of human endeavor has evolved a drastic change in the voting process of democratic decision making(Komatineni & Lingala, 2020). The shift from the existing conventional voting systems to electronic voting system will enable faster, convenient and more reliable means of franchising citizen's voting rights even in remote voting centres. Presently, an electronic voting machine is widely used, which has extensively reduced counting times as compared to the traditional ballots system (Perera & Patel, 2019)(Gomez-barrero et al., 2022). According to the authors, the mechanism would reduce time, expenses, and other unwarranted human effort.

Facial recognition and biometric authentication systems have gained increasing importance in today's society, mostly in electronic voting and other areas of wide applications ranging from access controls to secure systems (Shibel, Ahmad, Musa, & Yahya, 2022) (Choi & Lee, 2020). The biometric system provides a safe way to access private services and eliminates the need to carry a card, or to keep track of several passwords within election activities. On the contrary, facial recognition system is a tool used to identify users through ID verification services by comparing a human face from a digital image or video frame against a database of faces (Olaniyi et al., 2022). It has proved according to Hopal et al. (2021) to be most dependable and efficient biometric identification method when compared to other types.

The use of parametric authentication with facial recognition becomes imperative to facilitating a secured

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 7, Issue 8, pp 141-147, August-2023

https://doi.org/10.47001/IRJIET/2023.708018

voting system with high degree of privacy and proper voters' authentication transparency in the present age of increasing human population and societal challenges(Hu & Hu, 2021). Thus reducing the burden of litigation and indeterminate waste of time and other natural resources.

Consequently, this study attempts to characterize and propose the use of token with facial recognition as a parametric deep authentication base approach for an improved electronic voting in Nigeria. It is aim at enhancing the result accuracy, confidence building among the stakeholders and reduction in both economic materials and queuing time.

The remainder of the paper is organized as follows. In section 2, some of the contributions made in this research area so far are reviewed. The methodology of the research is presented in section 3 while section 4 presents the results and discussions of the study. Section 5 further provides the conclusion of the work and open issues.

II. LITERATURE REVIEW

Several studies on electronic voting; facial recognition and biometric authentication techniques for e-voting and its related electioneering architecture have been carried out over the years. Some of such literatures are reviewed and presented subsequently.

The work in Olaniyi et al. (2022) developed a distributed e-voting system that solve the problems of vote-rigging, voter impersonation, and vote falsification. In the study a combination of multifactor authentication (MFA) and blockchain techniques was used to secure the electronic voting. They demonstrated that the Combination of a facial recognition algorithm and RFID techniques did authenticate and authorize voters to participate in the election process. The MFA yielded a 0.1% false acceptance rate and a 0.8% false rejection rate for 100 voters, respectively. Though the developed system was observed to have less data reliability in full implementation. Similarly, Najam, Shaikh, and Naqvi (2018) proposed a novel hybrid based electronic voting system. Here, the authors used two voter verification techniques of finger print and facial recognition to give better results in comparison to single identification based systems. Cascaded machine learning based classifiers was further used to compare the features extracted from the biometric template that was pre-stored in the election regulatory body database. An accuracy of 91% was achieved. However, longer time to complete the voting process was a major drawback to the proposed system.

Vignesh et al. (2022) subsequently proposed an e-biometric voting machine that prevented fake votes using biometric validation. Two-step verification process was used and duly implemented using OTP as a parametric authentication data. However, the proposed system was not implemented with facial recognition techniques for enhanced voters' security and minimum queue time.

In Komatineni and Lingala (2020) the use of a secured and robust electronic voting system based on popular machine learning with facial recognition algorithms was demonstrated. The biometric authentication methodologies adopted had a secured voting system with face detection and bio-metric authentication. Following this development, Mansingh, Titus, and Devi (2020) studied the comparative importance of security measures in e-voting process. According to the study, the RFID and IoT (Internet of Things) were used to improvise the security mechanisms in electronic voting system. RFID tag was used in place of voter ID, the tag was scanned and matched with the fingerprints collected in the Aadhar database.

A machine learning model for automatic facial recognition in the e-voting systems was presented in Hopal et al. (2021). A recurrent neural networks algorithm was fully adopted in the research. It finds suitable application in facial recognition with improvement in increased accuracy and human errors reduction. While a framework for enhanced transparency and auditability in electronic voting system was conducted in Pawlak and Poniszewska-Marańda (2021). The work developed blockchain technology in cascade of intelligent agents and multi-agent system concept for Auditable Blockchain Voting System (ABVS). The proposed model used integrated e-voting process with blockchain technology for end-to-end verifiable e-voting process.

Perera and Patel (2019) on the other hand introduced a face-based multiple user active authentication with extreme value theory for modeling the distributions of electronic voting process. The authors further used an algorithm to estimate the parameters of extreme value distributions that demonstrated an effectiveness on the data set authentication. Also, Oke et al. (2021) presented multifactor authentication technique using fingerprint biometrics and enhanced cryptographically secured smart card to provide a more secure e-voting system's authentication. The technique involves the combination of an enhanced Feistel block cipher and first moment feature extraction technique. The results obtained from experimental simulation shows the viability of the developed technique to avert common problems encountered in voters' authentication during the electioneering process in a digitally divided democratic environment.

Subsequently, Ibitoye, Aworinde, and Adekunle (2022) developed a Facial Recognition Electronic Voting System powered by Blockchain Technology. The proposed election

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 7, Issue 8, pp 141-147, August-2023

https://doi.org/10.47001/IRJIET/2023.708018

engineering architecture were decentralized with improved security features for transparency, verifiability, and accountability for each vote count. The developed method had the capability to discard the intended fraudulent actions from election activities while facilitating privacy, convenience, eligibility and satisfactory voters' right. In the light of this, Shibel et al. (2022), noted the prevailing increasing importance of face recognition systems in today's society. According to the authors, its vital used in electronic voting and other areas demonstrated the wide applications in access controls and secure systems of electronic devices.

Consequently, Behrainwala (2022) deliberated on smart voting mechanism using facial recognition and verification. The author developed a computerized voting system to make the online voting election process more secured and user friendly. Furthermore, Danwar, Mahar, and Kiran (2022) proposed the framework of an e-voting system with blockchain ledger technology via facial recognition. The study linked the National Database and Registration Authority (NADRA) database for enhanced voter's validation. Voters and voting stations, real time of vote casting, network bandwidth were used to process and depict the results.

III. METHODOLOGY

This paper uses a prototyping method in designing an election facial recognition and biometric interface. Data for the study was gathered from Independent National Electoral Commission (INEC) state office Owerri. This data was analyzed using the Computer Package for Social Sciences (SPSS) version 23 and Excel Spread Sheet. Continuous and categorical data were analyzed using descriptive statistics. The prototyping method applied here aims at lessen the design faults and get rid of undesirable elements from the first design phase. In this case, we ensured that each step of election module was first finished in its entirety before moving on to the next module. The model process is an iterative, trial-and-error process that involves both the developer and the end users and allows testing to begin after the entire system development is completed. The system was designed to ensure effective voter registration and verification based on voters' expectations and existing electoral regulations in Nigeria.

i) Research Design: In the design and execution of the face recognition system, we adopted six fundamental phases in the digital image processing. The phases are the image acquisition (IA),image pre-processing (IP), image segmentation(IS), image representation (IR), image description (ID), and image recognition (IRe). We used the mage acquisition to obtain a digital picture and the image pre-processing to make the image better in ways that increases the likelihood that the other operations will be successful. The image segmentation was applied in dividing an input image into its individual objects of the digital image configuration. The next phase of mage representation was used to put the input data in a format that can be processed by the computer. While the image description distinguishes one class of objects from another and made it necessary to extract the features that produce quantitative information of interest. Finally, the image recognition helped in giving the image object a name based on its provided details.

ii) Proposed System: The system was designed to first, logs in as a master admin who registers and gives access privileges to other admin officers and staff members. Registered staff members were given the privilege of registering all eligible voters while ensuring that voters' faces was captured in digital image alongside other voter parameters. In this case, for every successfully registered voter, a unique voter ID called a token is generated in form of a parametric number. This was used by the system to hasten the process of voter verification. The user case diagram of the proposed system is shown in Fig. 1, with two active key players of admin and the voter.

The various activities for execution on the proposed system and their relationship are revealed. The admin login and register the voters, verify voters, view the details, store information and log out, while the voters can provide the face-print and receive notification as token for authentication.

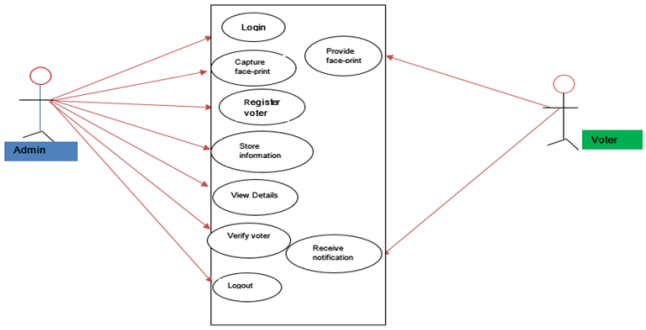

Figure 1: Use Case Diagram of the Proposed System

At the point of voter verification, a unique PIN (in the form of Voter ID number) generated during the registration stage will be used to reference the stored template of the individual. When a voter attempts to authenticate, the voter ID number will be entered in the first instance, which instructs the system of the particular template to retrieve for comparison. The live sample would then be compared against the retrieved template and a match or no-match scenario would result. In this way the system is actually verifying that the individual is who he/she claims to be. Indeed, for every verified voter, a unique token will be generated that automatically delivers to

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 7, Issue 8, pp 141-147, August-2023

https://doi.org/10.47001/IRJIET/2023.708018

the voter's phone number via SMS gateway provider, in order to avoid incidences of multiple voting.

iii) Software Requirement Specification: A tokenized biometric authentication was used as the key expected functionality in the system requirements of the developed model. The system requirements were categorized into two namely:
   a) Functional requirements
   b) Non-functional

Functional requirements: the list of functional requirements includes the services that the system should deliver, as well as the response to specific inputs and behavior in specific situation such that the system:

- Register the voters during enrolment stage
- Authenticate and verify the voters at the verification stage
- Generate and transfer a unique token for each verified voter to his/her phone.

Non-functional requirements: These include the accuracy, speed, flexibility, manageability and reliability.

iv) Model Precondition and Post-Condition: The actors are structured in the system with the required condition of functionality well built in the model. The whole process of the face-print capture in Table 1 and the receiver notification in Table 2 is suited properly for flexibility, accuracy and reliability. In Table 1, the actors are the admin.The administrator captures the face of the voter for during registration. The precondition and the post-condition are performed with reference to the basic course of action (BCA) that the admin must click on the web camera button which is in-built, then the face is displayed on the camera screen and the face is stored automatically on the system. In Table 2, the actors are the voters. The voter receives authentic information from his/her phone to clear him from election immediately Token is generated. The precondition and the post-condition are performed similarly with reference to the BCA that the voter receives authentication information from the phone and the verified identity shows an evidence of his/her eligibility to cast vote.

Table 1: Capture Face-Print

Use case Name	Capture Face-Print
Actor(s)	Admin
Description	The administrator captures the face for voter registration
Precondition	Admin used his/her style of capturing the face
Post-condition	The admin snapped a photo of the voter for his/her recognition
Basic Course of Actions (BCA):	
1) The admin click on the web camera button which is in-built 2) The face is displayed on the camera screen 3) The face is stored automatically on the system	

Table 2: Receive Notification

Use case Name	Receive Notification
Actor(s)	Voter
Description	The voter receives authentic information from his/her phone to clear him from election immediately token is generated
Precondition	The voter has confirmed his/her eligibility
Post condition	The voter keeps his/her confirmation confidentially for voting
Basic Course of Actions	
1) The voter from his/her phone receives authentication information from the system 2) The verified identity shows an evidence of his/her eligibility to cast vote	

IV. RESULTS AND DISCUSSION

In this section, the result obtained at different stages of this study is presented. First is the output screen presented in Figure 2, which shows the results of the system implementation and the model functional interface.

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 7, Issue 8, pp 141-147, August-2023

https://doi.org/10.47001/IRJIET/2023.708018

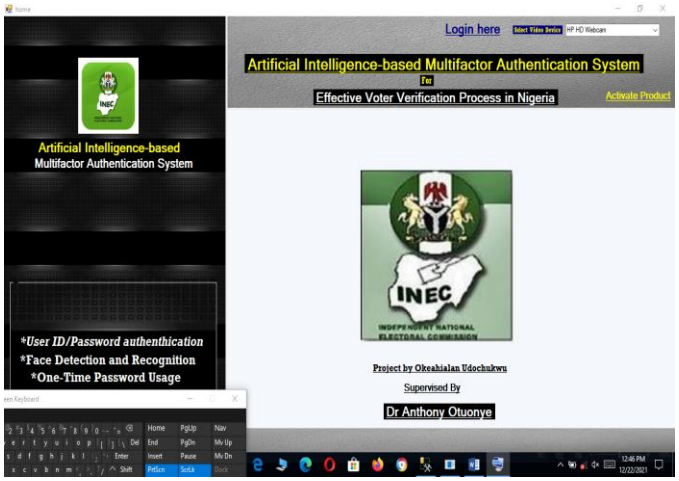

Figure 2: System Home Page

The home page of the developed model is built with unique features of multifactor techniques such as the user ID/Password authentication, Face Detection & Recognition and One-Time Password. These features are encapsulated for effective voter verification process.

Next is the login page represented in Figure 3, it is used to validate the authorized users of the system as well as restrict access to unauthorized users. This functionality facilitates secured voter registration and voter verification.

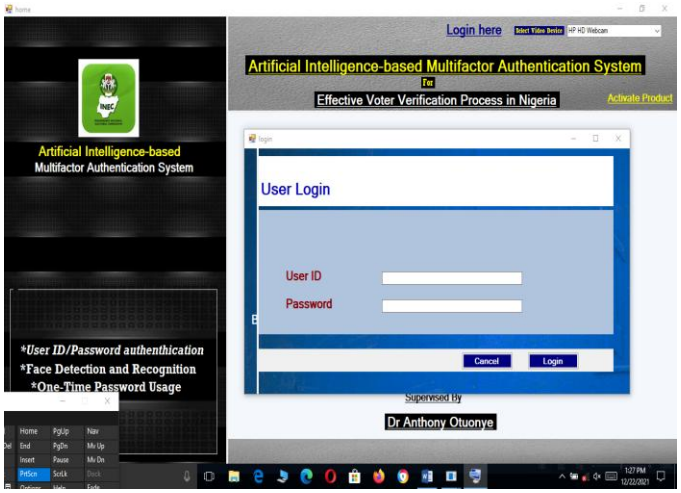

Figure 3: System Login Page

The main feature of the model developed is the Token Verification Page (tvp) with Voters' Registration Page (vrp) in Figure 4. This features promotes the confidentiality, scalability and the overall reliability of the system. Token verification page allows a verified voter with the correct Token to cast his/her vote seamlessly. Thereby help to prevent unauthorized access of user accounts and enhance time benefit effectiveness of the election administration. The voter's details are fully displayed after correct data detection and matching using facial recognition mechanism built in the system.

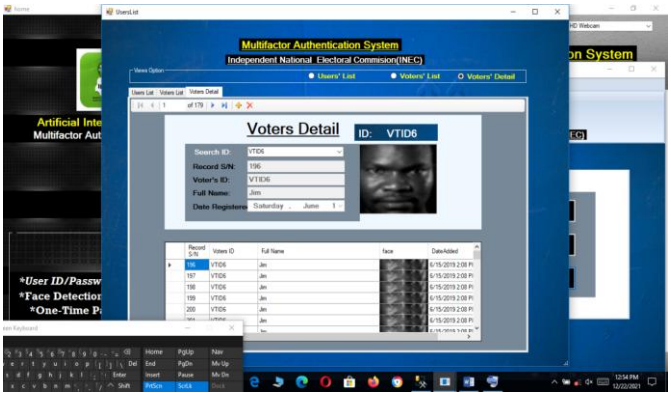

Figure 4: Token Verification and Voters' Registration Page

Furthermore, the system was deployed into testing and use among various INEC personnel and other recipients. A questionnaire was designed to collect the appropriate responses from the respondents with specific focus on the face detection operation ability and accurate registration and verification scenarios of voters. The confidence rating from the various election stakeholders on these key functionalities were populated and the results of this use case testing are presented in Figure 5 and Figure 6 respectively.

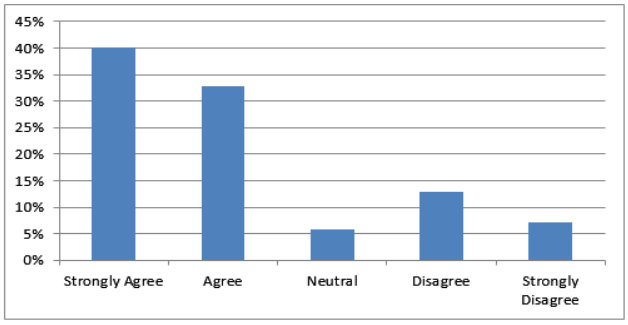

Figure 5: System Life Face Detection

A total of (40%) of the respondents strongly agree that the developed system is capable of performing life face detection. (32.9%) further agreed while (5.9%), (12.9%), (7.1%) of the respondents were the neutral, disagree, and strongly disagree respondents respectively.

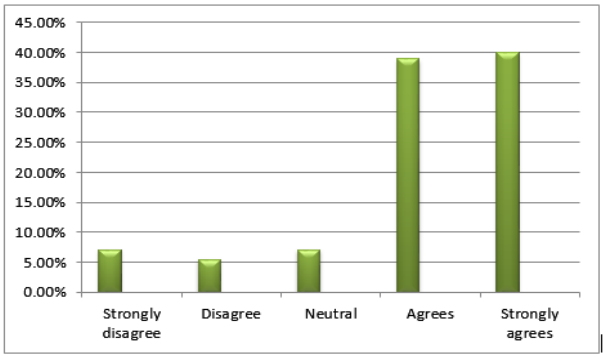

Figure 6: Proposed System Accurate Registration and Verification

ISSN (online): 2581-3048
Volume 7, Issue 8, pp 141-147, August-2023
https://doi.org/10.47001/IRJIET/2023.708018

A higher proportion of respondents 34(40%) strongly agrees that the system is highly efficient in registering and verifying a voter; followed by 33(38.9%), that agrees; 6(7.1%) are neutral while 5(5.5%) and 6(7.1%) disagrees and strongly disagrees respectively. The highest percentage of the respondents (40%) is enough to guarantee the efficiency of the system based on the total number of respondents considered.

Finally, the time effectiveness of the proposed system was also tested. The result is presented in Figure 7.

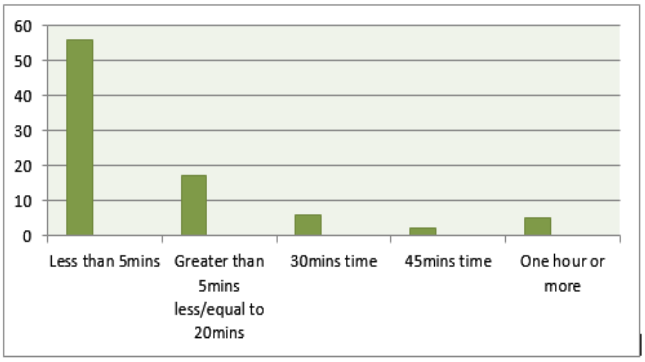

Figure 7: Proposed System Time of Face Recognition

The proposed system operates in less than 5 minutes timeline. This was an improvement from the existing system that takes large more than 5 minutes for face recognition. Thus, the system is both time benefit and reliable for use.

V. CONCLUSION

This paper presents the development of a parametric token-based biometric authentication system that guarantees efficient voter registration and verification processes in Nigeria involving facial recognition of registered voters. The user requirements for effective voter verification based on voter expectations and electoral regulation in Nigeria were accurately ascertain. The system is capable of capturing faces of voters alongside other parameters at point of voter registration in less than 5 minutes time duration. It has demonstrated improved key election parameters of reliability and time effective using a unique token functionality. However, the need to integrate a scalable and dynamic artificial intelligence driven software for more optimal performance of the system is recommended for further improvement.

REFERENCES

[1] Behrainwala, A. (2022). Smart Voting System Using Facial Recognition. *International Journal for Research in Applied Science and Engineering Technology*. https://doi.org/10.22214/ijraset.2022.39810

[2] Choi, J. Y., & Lee, B. (2020). Ensemble of Deep Convolutional Neural Networks with Gabor Face Representations for Face Recognition. *IEEE Transactions on Image Processing*. https://doi.org/10.1109/TIP.2019.2958404

[3] Danwar, S. H., Mahar, J. A., & Kiran, A. (2022). A Framework for e-Voting System Based on Blockchain and Distributed Ledger Technologies. *Computers, Materials and Continua*. https://doi.org/10.32604/cmc.2022.023846

[4] Gomez-barrero, M., Drozdowski, P., Rathgeb, C., Patino, J., Todisco, M., Nautsch, A., … Jul, C. Y. (2022). Biometrics in the Era of COVID-19 : Challenges and Opportunities. 1–15.

[5] Hopal, P., Kothar, A., Pimpale, S., More, P., & Patil, J. (2021). A Survey on Performing E-Voting through Facial Recognition. *International Journal of Scientific Research in Science and Technology*. https://doi.org/10.32628/ijsrst218318

[6] Hu, W., & Hu, H. (2021). Dual Adversarial Disentanglement and Deep Representation Decorrelation for NIR-VIS Face Recognition. *IEEE Transactions on Information Forensics and Security*. https://doi.org/10.1109/TIFS.2020.3005314

[7] Ibitoye, A. O. ., Aworinde, H. O., & Adekunle, E. T. (2022). An Enhanced Multi-Level Authentication Electronic Voting System. *International Journal of Applied Sciences and Smart Technologies*. https://doi.org/10.24071/ijasst.v4i2.5237

[8] Komatineni, S., & Lingala, G. (2020). Secured E-voting System Using Two-factor Biometric Authentication. *Proceedings of the 4th International Conference on Computing Methodologies and Communication, ICCMC 2020*. https://doi.org/10.1109/ICCMC48092.2020.ICCMC-00046

[9] Mamokhere, J., & Mabeba, S. J. (2022). A request for e-voting system in South Africa: A case of 2019 national elections. *Journal of Public Affairs*. https://doi.org/10.1002/pa.2338

[10] Mansingh, P. M. B., Titus, T. J., & Devi, V. S. S. (2020). A Secured Biometric Voting System Using RFID Linked with the Aadhar Database. *2020 6th International Conference on Advanced Computing and Communication Systems, ICACCS* 2020. https://doi.org/10.1109/ICACCS48705.2020.9074281

[11] Najam, S., Shaikh, A. Z., & Naqvi, S. (2018). A Novel Hybrid Biometric Electronic Voting System: Integrating Finger Print and Face Recognition. *Mehran University Research Journal of Engineering and Technology*. https://doi.org/10.22581/muet1982.1801.05

ISSN (online): 2581-3048
Volume 7, Issue 8, pp 141-147, August-2023
https://doi.org/10.47001/IRJIET/2023.708018

[12] Nguyen, H. P., Delahaies, A., Retraint, F., & Morain-Nicolier, F. (2019). Face Presentation Attack Detection Based on a Statistical Model of Image Noise. *IEEE Access.* https://doi.org/10.1109/ACCESS.2019.2957273

[13] Oke, B. A., Olaniyi, O. M., Aboaba, A. A., & Arulogun, O. T. (2021). Multifactor authentication technique for a secure electronic voting system. *Electronic Government.* https://doi.org/10.1504/EG.2021.115999

[14] Olaniyi, O. M., Dogo, E. M., Nuhu, B. K., Treiblmaier, H., Abdulsalam, Y. S., & Folawiyo, Z. (2022). A Secure Electronic Voting System Using Multifactor Authentication and Blockchain Technologies. *In EAI/Springer Innovations in Communication and Computing*. https://doi.org/10.1007/978-3-030-89546-4_3

[15] Panizo Alonso, L., Gasco, M., Marcos Del Blanco, D. Y., Hermida Alonso, J. A., Barrat, J., & Alaiz Moreton, H. (2021). E-Voting System Evaluation Based on the Council of Europe Recommendations: Helios Voting. *IEEE Transactions on Emerging Topics in Computing.* https://doi.org/10.1109/TETC.2018.2881891

[16] Pawlak, M., & Poniszewska-Marańda, A. (2021). Trends in blockchain-based electronic voting systems. *Information Processing and Management*. https://doi.org/10.1016/j.ipm.2021.102595

[17] Perera, P., & Patel, V. M. (2019). Face-based multiple user active authentication on mobile devices. *IEEE Transactions on Information Forensics and Security*. https://doi.org/10.1109/TIFS.2018.2876748

[18] Shibel, A. M., Ahmad, S. M. S., Musa, L. H., & Yahya, M. N. (2022). Deep learning detection of facial biometric presentation attack. Life: *International Journal of Health and Life-Sciences.* https://doi.org/10.20319/lijhls.2022.82.0118

[19] Venkata Ramakoteswararao, T., & Bhaskarrao, Y. (2020). Face recognition system for fare elections. *International Journal of Advanced Science and Technology*.

[20] Vignesh, B., Sricharan, P. P., Shankrith Chokkalingam, S., Bhuvana, J., & Bharathi, B. (2022). E-Biometric Voting Machine. *Lecture Notes in Electrical Engineering*. https://doi.org/10.1007/978-981-16-4625-6_50

Citation of this Article:

Udochukwu Okeahialam, Anthony I. Otuonye, Mathew E. Nwanga, "Parametric-Based Facial Recognition Technique for Improved Electronic Voting System" Published in *International Research Journal of Innovations in Engineering and Technology - IRJIET*, Volume 7, Issue 8, pp 141-147, August 2023. Article DOI https://doi.org/10.47001/IRJIET/2023.708018

****

