Journal of Innovative Image Processing (JIIP) (2021)
Vol.03/ No. 03
Pages: 255-268
https://www.irojournals.com/iroiip/
DOI: https://doi.org/10.36548/jiip.2021.3.007

Construction of Efficient Smart Voting Machine with Liveness Detection Module

Yasir Babiker Hamdan[1], A. Sathesh[2]

[1]International University of Africa (IUA), Khartoum, Sudan
[2]Department of Electronics and Communication Engineering, Eritrea Institute of Technology, Eritrea

E-mail: [1]yasir20ap@iua.edu.sd, [2]sathesh4you@gmail.com

Abstract

Voting is now governed by regulations that specify how a person's choices may be communicated and their desires can be realized. This study proposes an electronic voting machine (EVM) as an alternative for traditional voting methods, which may include the manual utilization of only microcontroller-based circuits. With the identified fingerprint liveness, the proposed technique will make voting considerably easier, more effective, and less likely to result in fraud. The suggested model will support and advance the trustworthiness of all votes and it will also assist in streamlining the counting and verification process. It is difficult to demonstrate that an advanced voting system has been properly designed since several critical criteria must be satisfied. Poll results should be kept private in the database in order to preserve the data. The voting process must also show the votes obtained by the respective candidates. The proposed authenticated voting machine can be applied to the local area elections in order to speed up the process and make the election process more transparent. To maintain its theoretical strength, the proposed research idea needs further study. The model employs radio frequency and fingerprint recognition to maintain the protection.

Keywords: Smart voting machine, liveness detection module

ISSN: 2582-4252 (online)
Submitted: 05.07.2021
Revised: 30.08.2021
Accepted: 03.09.2021
Published: 13.09.2021

1. Introduction

In other terms, an electronic voting system is a collection of electronic devices used to assist in the counting and casting of votes. To vote over the internet, a web application or a smartphone application known as internet voting is utilized. The major purpose of this article is to investigate the remote e-voting option, often known as e-voting since it eliminates the need for election supervisors to monitor each vote counting via the internet and smartphones [1-3].

The ability to verify votes must be included in every election instrument that has been used to cast ballots if voters have confidence that their votes were properly recorded. This is particularly true when it comes to distant e-voting through mobile phones. This is particularly relevant by making sure that votes are casted as intended without mistakes since this was a common problem with outdated voting technology used in the recent United States elections [4-7].

With the increased involvement of technology, many spoofing fingerprints are detected. In other words, there is only one way to identify liveness, and that will be implemented via liveness detection. Liveness detection will identify the living moment or any functional information for the person or any functional information in the system [8].

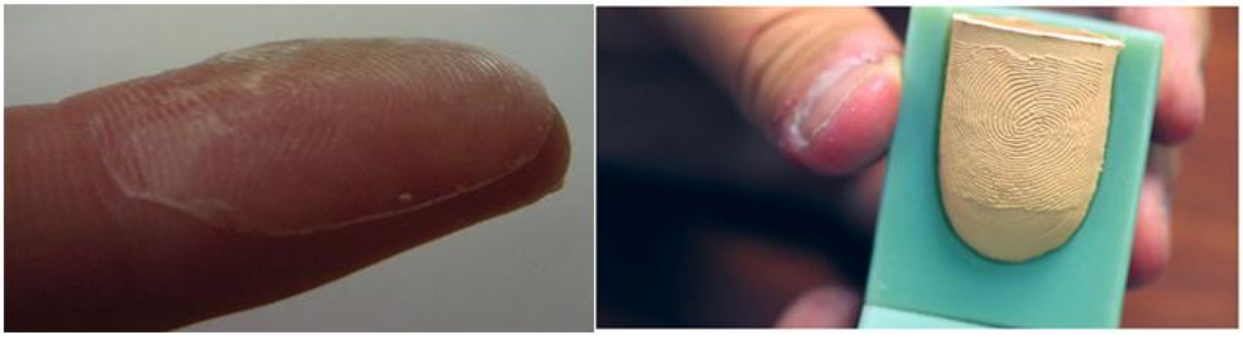

Figure 1. Fingerprint Spoof Chances

ISSN: 2582-4252 (online)
Submitted: 05.07.2021
Revised: 30.08.2021
Accepted: 03.09.2021
Published: 13.09.2021

Only three candidates may win a single election under the voting method has been discussed. A separate voting system is utilized for each post if there are more posts. The election booth is split into numerous blocks with each block having one booth-level operator (BLO) in charge of voting. The fingerprint data of students will be used to build the college database. This stage requires an internet connection, preferably Wi-Fi [9-12].

In India, the voting system plays a significant role during elections due to the democratic nature of the country. Electronic voting devices are traditionally used in India require more personnel, consume extra time, and also less reliable. While we all know that elections are an important aspect of democracy, selecting a candidate is a crucial part of the process. The developing country like India is spending heavily in upgrading the entire voting system in order to assist the people. To strengthen the democratic process in India, the voting system should be honest, transparent, and secure [13-15].

2. Organization of the Research

The remaining part of the research paper is organized as follows: Section 3 summarizes the current research works available on the design of smart electronic voting machines. The proposed smart voting system is discussed in Section 4. Section 5 contains the calculated findings along with an explanation. The last portion of this article discusses about the potential challenges faced by the smart voting machines.

3. Preliminaries

The secured voting system with fingerprint, face, and iris verification proposed by Kavitha et al ensures the greatest level of voting security. To begin, the voter must enter his or her fingerprints on the fingerprint scanner. MatLab is the program used to compare and verify the input and trained data. All input data is compared to the database that has been previously saved. If any step of verification fails, the system will deem the user to be a phony voter. Each step should be validated correctly and the input data should be compared to the stored database. The voter will next see the candidate's names and may vote for the preferred candidate. This method improves the security of the voting process and it is simple to use [16].

A group of researchers led by Ashwini Ashok Mandavkar, have used OTP verification for utilizing mobile-based face recognition for voting. First, a voter would use the Android mobile phone's face recognition feature to build a database of voters. It is very necessary to have an internet connection for this system to work. In order to register for voting, the voter has to go through an application [17].

B Madhuri et al have discussed about the secured smart voting system, which uses the Aadhar database. Most of this study explores how India has cut its voting rate. This article suggests a solution to the outlined issue by creating a mobile application that is both simple and safe. Since it is built on a mobile application, it is far more secure than a web-based voting system [18].

J. Deepika et al. have written an article by discussing about a biometric-based voting system. In a business context, biometrics is defined as a unique identifier, such as DNA and Iris. In this system, IoT technology is used for performing server management and to upgrade the voting information up to current. Here is a complete list of the voting devices that are linked to the same server. Each constituency has its server. Initially, fingerprint verification takes place. After the biometric system has been proven reliable, it will consult the database to make sure it has not changed [19].

Devi et al. have examined the features and utilizes multimodal biometric and biometric system modules, methods, and the associated difficulties. This method utilizes several sensors to collect biometric data for a single characteristic that contains many samples. The company is using

ISSN: 2582-4252 (online)
Submitted: 05.07.2021
Revised: 30.08.2021
Accepted: 03.09.2021
Published: 13.09.2021

cryptographic methods like RSA and AES to encrypt the biometric sample by ensuring the security and safety [20].

Research Gap

While there is still the possibility of voting fraud, the current approach is used with less transparency. One of the most serious issues confronting the current election voting process is voter authentication, voting process security, and voter information security. Even if they had voter IDs from previous addresses, many do not have them at their present addresses. It is impossible for them to travel to their polling stations; therefore they will not be able to cast their important vote. As a result, a huge part of our residents do not vote, which is why our voting percentage has decreased. While working to fix the problem, our administration is also committed to finding the best possible solution. The majority of our project will be devoted to developing a safe electronic voting system for liveness detection [8].

4. Proposed Method

4.1 Input Module

A fingerprint reader and signal conditioner circuit serve as the input module since they condition the signal and reduce the amount of data that flows between electronic devices. Every RFID tag is a unique device that tracks the student information. In this reader, the information about the RFID tag will be saved. The technology utilizes a contactless communication module (reader/writer) to identify the voter [21]. This highly integrated RFID transmission module integrates both serial and Ethernet communication to interact with the microcontroller.

ISSN: 2582-4252 (online)
Submitted: 05.07.2021
Revised: 30.08.2021
Accepted: 03.09.2021
Published: 13.09.2021

4.2 Fingerprint Module

This module comprises of a fingerprint scanner as well as a portion for fraud analysis. This portion of the analysis is often overlooked in many research works, which is unfortunate. This analysis part is concerned with the collection and processing of fingerprint pictures, as well as the identification of liveness in fingerprint images. This effort considerably generates more significant results than other conventional ways of producing results [22]. The fingerprint module includes optical fingerprint sensors, a fast DSP processor, a quick fingerprint algorithm, a high-capacity FLASH memory, and other hardware and software components for stability, simple layout, fingerprint entry, image processing, and more. Fingerprints are used to identify and verify suspects. When a person vote, that particular person’s unique fingerprint is scanned and the database is checked for registration. To connect the DSP to the microcontroller, it is connected to the microcontroller via a TTL serial cable. It creates fingerprint packets for tracking.

4.2.1 Fraud Analysis

A low-pass filter is used to look at the continuously changing picture. Low-pass and high-pass filtering methods are the currently utilized filter techniques. To remove the noise from the original pictures, the high pass filtering methods are used, which in this case is subtracting the noise-free images to get the pure image. Figure 2 shows the proposed framework.

4.2.2. “Liveness” Detection in Fingerprint

This process is used to filter out the noise and unnecessary information from the picture. Fake and genuine fingerprint "liveness" analysis was evaluated in a real-time situation and the hypothesis conditions were determined to be true. Spatial resolution is one of the most essential

ISSN: 2582-4252 (online)
Submitted: 05.07.2021
Revised: 30.08.2021
Accepted: 03.09.2021
Published: 13.09.2021

factors to consider when classifying "liveness" fingerprint detection. To evaluate various functions at different scaling levels of the interpolation function, image reduction is used [23] [8].

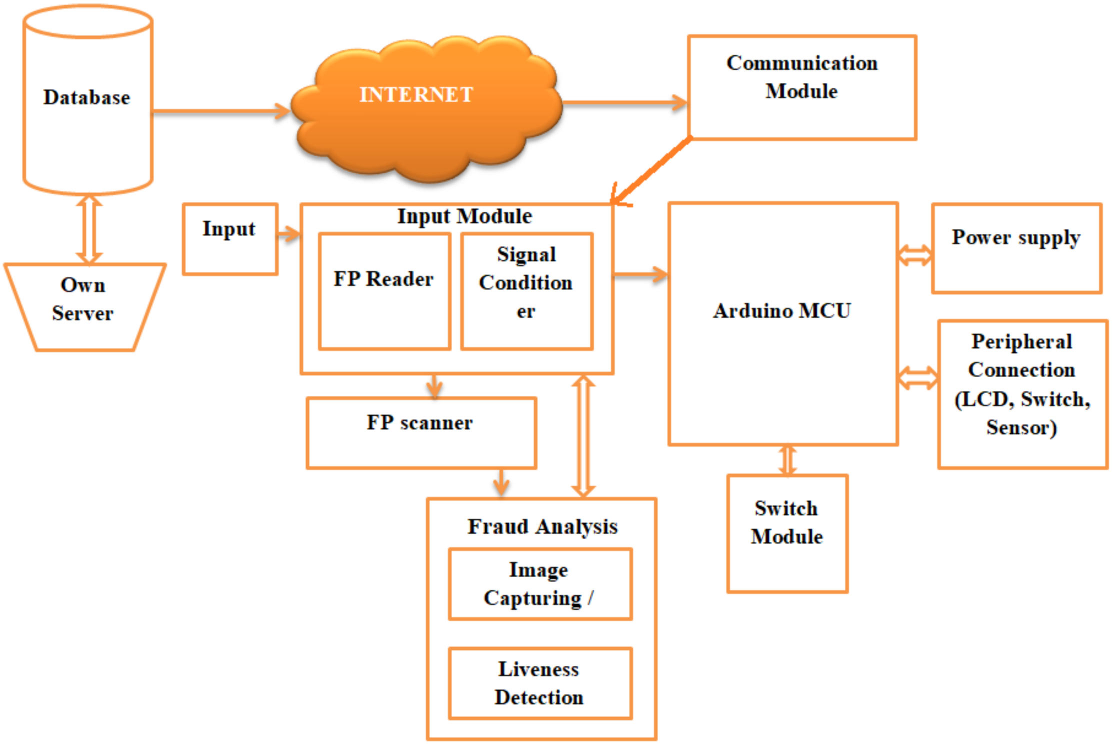

Figure 2. Proposed Framework

4.3 Wi-Fi Module

The Wi-Fi module is used to establish a connection between the EVM and external data sources. This chip can connect microcontrollers to a Wi-Fi network and make simple TCP/IP communications. Many IoT devices have the SoP module, which is frequently developed and used for IoT embedded applications. A sequence of AT commands is necessary for microcontrollers to communicate with such a communication module. [24].

ISSN: 2582-4252 (online)
Submitted: 05.07.2021
Revised: 30.08.2021
Accepted: 03.09.2021
Published: 13.09.2021

4.4 Switch Module

Switch module consists of LCD crystal display, buzzer, and push buttons. In this instance, LCD is being used to display notifications for casting their vote. Four wires link the 12C liquid crystal display: GND, VCC, SDA, and SLC. Because of the height, two lines may display 16 characters per row. This LCD screen bridges the gap between the user and the Arduino by showing necessary programmed messages such as when to expose the ID card, when to place the finger on the screen, and so on. When the authentication is successful, the system will enable the voter to vote by hitting one of the three candidate buttons. If the LED blinks once, the message will be shown on the same LCD showing that the vote was successful [25].

5. Results & Discussion

Unlike conventional voting, in electronic voting, the results of the voting can be declared as soon as the voting machine completes the next step; in our case, the results can be found at any point during the voting process. The circuit model has been shown in figure 3.

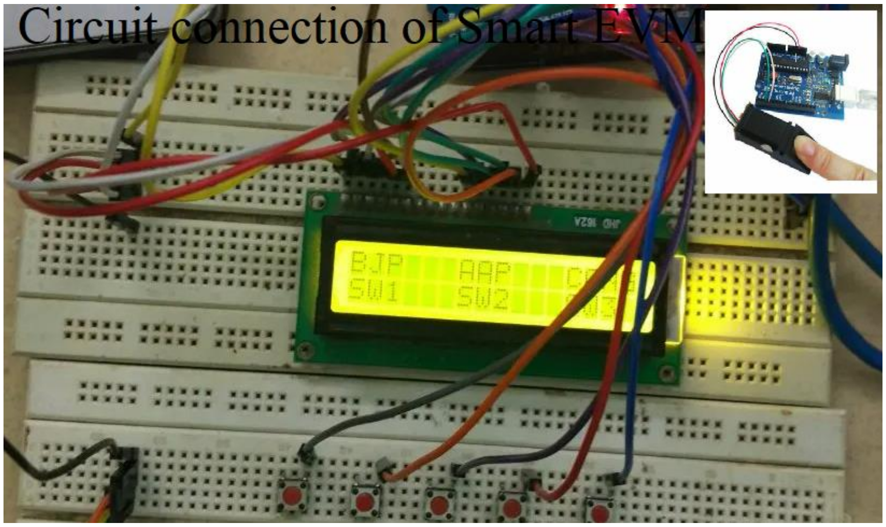

Figure 3. Overall Circuit of Smart Election Voting Machine with Fingerprint Reader

All votes must be manually counted in traditional voting, whereas electronic voting does not require any manual counting. This is due to the fact that we have connected the "FINAL RESULT" button to Arduino's external interrupt pin, which is located in the interrupt pin. When the "FINAL RESULT" button is pressed, the controller is interrupted and the interrupt process is conducted on the controller, as stated in the "Interrupt" section. Table 1 includes the computed performance metrics data.

Table 1. Computed Performance Metrics

S.No	Method	Accuracy (tested with No.of iteration)	Efficiency (tested with No.of iteration)	Total Response time (Sec)
1	Traditional Microcontroller EVM	89.34%	74%	50
2	Microcontroller based Smart EVM	80.98%	80%	60
3	Proposed EVM fingerprint analysis with liveness detection	95.34%	96%	94

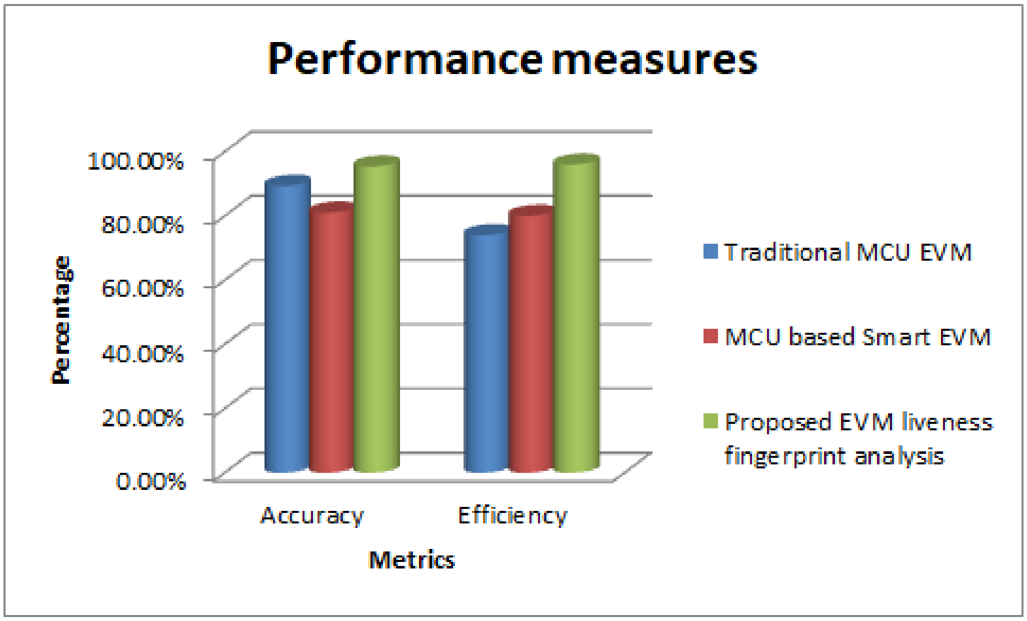

Figure 4. Performance of Overall System

ISSN: 2582-4252 (online)
Submitted: 05.07.2021
Revised: 30.08.2021
Accepted: 03.09.2021
Published: 13.09.2021

Before getting started, the LCD must be initialized and its operating mode is selected. After the data is extracted from the memory address, where each of the candidates' votes is stored, translated to ASCII hex code, and supplied to the LCD, the screen should be updated with the following results: The delay between each block of data is equal to a tiny amount. Using the delay method of delivering data to the LCD rather than using the busy flag checking technique will reduce these problems. Figure 4 shows the overall performance metrics of the proposed model.

During this time, the entire "FINAL RESULT" stays on the screen. The input data is shown for 60 seconds, after which the screen is cleaned and the entered data's name is displayed and performed again. The process is performed 3 times then it gets repeated back to the main program such as executing from the main program. The computation time is a bit larger than other traditional microcontroller units (MCU), which are shown in table 1. The proposed system has achieved good efficiency than other traditional methods.

6. Conclusion

As a consequence, the developed module produces an efficient outcome for bogus fingerprint pictures. Apart from that, it has been estimated that the suggested module's efficiency and accuracy are much higher than other conventional modules. However, with the proposed fraud analysis module, we are seeing an issue with overall response time. The planned work should be modified so that it makes use of less electronic equipment to decrease the response time throughout the course of its execution. The proposed work establishes the principles, which will guide us in the implementation of a smarter voting machine. But these must be researched further to make sure that the proposed model is both technically and operationally feasible. Additionally, the system enables only one post to be elected at a time. It can be designed to be used for any number of elected posts at once. These devices are flexible, secured and the data can be stored in the cloud and the voting process will run more quickly on automated lists of new voters. An additional research work is required to develop the system into a versatile and adaptive one [26, 27].

References

[1] A Jagan, P Akila, and N Nasrin, "QR Code Based E-voting System Using an Android Smart Phones," International Journal of Emerging Technology in Computer Science & Electronics, vol. 13, no. 2, pp. 263-267, March 2015.

[2] Shakya, Subarna. "IoT based F-RAN Architecture using Cloud and Edge Detection System." Journal of ISMAC 3, no. 01 (2021): 31-39.

[3] P.S. Ghatol and N. Mahale, "Biometrics Technology Based Mobile Voting Machine," International Journal of Computer Sciences and Engineering, vol. 2, no. 8, pp. 45-49, August 2014.

[4] Smys, S., and Haoxiang Wang. "Security Enhancement in Smart Vehicle Using Blockchain-based Architectural Framework." Journal of Artificial Intelligence 3, no. 02 (2021): 90-100.

[5] S. Kimbi, Y. Nkansah-Gyekye, and K. Michael, "Towards A Secure Remote Electronic Voting in Tanzania Organizational Challenges," Advances in Computer Science: an International Journal, vol. 3, no. 5, pp. 122-131, September 2014.

[6] Lai, Kong-Long, and Joy Iong Zong Chen. "Development of Smart Cities with Fog Computing and Internet of Things." Journal of Ubiquitous Computing and Communication Technologies (UCCT) 3, no. 01 (2021): 52-60.

[7] M.R. Clarkson, S. Chong, and A.C. Myers, "Civitas: A Secure Remote Voting System," Cornell University, Technical Report 2007.

[8] Adam, Edriss Eisa Babikir. "Evaluation of Fingerprint Liveness Detection by Machine Learning Approach-A Systematic View." Journal of ISMAC 3, no. 01 (2021): 16-30.

ISSN: 2582-4252 (online)
Submitted: 05.07.2021
Revised: 30.08.2021
Accepted: 03.09.2021
Published: 13.09.2021

[9] Sivaganesan, D. "A Data Driven Trust Mechanism Based on Blockchain in IoT Sensor Networks for Detection and Mitigation of Attacks." Journal of trends in Computer Science and Smart technology (TCSST) 3, no. 01 (2021): 59-69.

[10] Singh, Sushil Kumar, Debjani Dey, and Sushanta Bordoloi. "Internet of Things Based Electronic Voting Machine." In International Conference on Intelligent Data Communication Technologies and Internet of Things, pp. 365-372. Springer, Cham, 2019.

[11] Bagde, Sejal, Pratiksha Ambade, Manasvi Batho, Piyush Duragkar, Prathmesh Dahikar, and Avinash Ikhar. "Internet of Things (IOT) Based Smart Switch." Journal of IoT in Social, Mobile, Analytics, and Cloud 3, no. 2 (2021): 149-162.

[12] Reddy, B. M. M., & Srihari, D, 2015, RFID Based Biometric Voting Machine Linked To Aadhaar For Safe And Secure Voting. International Journal of Science, Engineering and Technology Research (IJSETR). 4(4), 995–1001

[13] Suma, V., and Wang Haoxiang. "Optimal Key Handover Management for Enhancing Security in Mobile Network." Journal of trends in Computer Science and Smart technology (TCSST) 2, no. 04 (2020): 181-187.

[14] Nishant, Potnuru Sai, Bhaskaruni Gopesh Krishna Mohan, Balina Surya Chandra, Yangalasetty Lokesh, Gantakora Devaraju, and Madamala Revanth. "Lexicon-Based Text Analysis for Twitter and Quora." In International Conference on Innovative Data Communication Technologies and Application, pp. 276-283. Springer, Cham, 2019.

[15] Chen, Joy Iong Zong, and P. Hengjinda. "Enhanced Dragonfly Algorithm based K-Medoid Clustering Model for VANET." Journal of ISMAC 3, no. 01 (2021): 50-59.

[16] Sharma, Ruchi, and Kiran Davuluri. "Security Analysis for Machine Learning and Image Processing Related Information Systems." In International Conference on Image Processing and Capsule Networks, pp. 135-147. Springer, Cham, 2020.

[17] Ms. Ashwini Ashok Mandavkar, Prof. Rohini Vijay Agawane,n“Mobile Based Facial Recognition Using OTP Verification for Voting System” 2015 IEEE International Advance Computing Conference (IACC).

[18] Madhuri, B., M. G. Adarsha, K. R. Pradhyumna, and B. M. Prajwal. "Secured smart voting system using aadhar." In 2017 2nd international conference on emerging computation and information technologies (ICECIT), pp. 1-3. IEEE, 2017.

[19] J. Deepika , S. Kalaiselvi , S. Mahalakshmi, S. Agnes Shifani, “Smart Electronic Voting System Based On Biometric Identification-Survey” 2017 Third International Conference on Science Technology Engineering & Management (ICONSTEM).

[20] R. Devi, P. Sujatha, “A Study on Biometric and Multi-modal biometric system modules, Applications, Techniques and Challenges” Proc. IEEE Conference on Emerging Devices and Smart Systems (ICEDSS 2017) 3-4March 2017, Mahendra Engineering College, Tamilnadu, India.

[21] Agarwal, Vartika, Sachin Sharma, and Piyush Agarwal. "IoT Based Smart Transport Management and Vehicle-to-Vehicle Communication System." In Computer Networks, Big Data and IoT, pp. 709-716. Springer, Singapore, 2021.

[22] Chatterjee, Runa, Rajdeep Chakraborty, and J. K. Mondal. "Design of Lightweight Cryptographic Model for End-to-End Encryption in IoT Domain." IRO Journal on Sustainable Wireless Systems 1, no. 4 (2019): 215-224.

[23] Nikam, R., Rankhambe, M., Raikwar, D., & Kashyap, A, 2014, Secured E-Voting Using NFC Technology. International Journal of Computer Science and Information Technologies, 5(6), 8325–8327.

[24] Haoxiang, Wang, and S. Smys. "Big Data Analysis and Perturbation using Data Mining Algorithm." Journal of Soft Computing Paradigm (JSCP) 3, no. 01 (2021): 19-28.

[25] Gangrade, Sakshi, and Srinath R. Naidu. "Measurement of Acid Content in Rain Water Using Wireless Sensor Networks and Artificial Neural Networks." In International

ISSN: 2582-4252 (online)
Submitted: 05.07.2021
Revised: 30.08.2021
Accepted: 03.09.2021
Published: 13.09.2021

Conference On Computational Vision and Bio Inspired Computing, pp. 598-605. Springer, Cham, 2019.

[26] Haoxiang, Wang, and S. Smys. "A Survey on Digital Fraud Risk Control Management by Automatic Case Management System." Journal of Electrical Engineering and Automation 3, no. 1 (2021): 1-14

[27] Mugunthan, S. R. "Wireless Rechargeable Sensor Network Fault Modeling and Stability Analysis." Journal of Soft Computing Paradigm (JSCP) 3, no. 01 (2021): 47-54.

Author's biography

Yasir Babiker Hamdan is presently working in International University of Africa (IUA), Khartoum, Sudan. His research is mainly focused on computer graphics, image processing, data mining, neural network algorithms and blockchain technologies.

A. Sathesh completed his master's degree in the year 2006 and has published several papers in national and international journals. His areas of interest include wavelets and multi-resolution transforms for image denoising. Currently, he is occupying an academic position in Eritrea after having worked in a reputed University in South India for the past 5 years. He is pursuing his research work in the area of complex wavelets for image approximations with a deep learning approach.