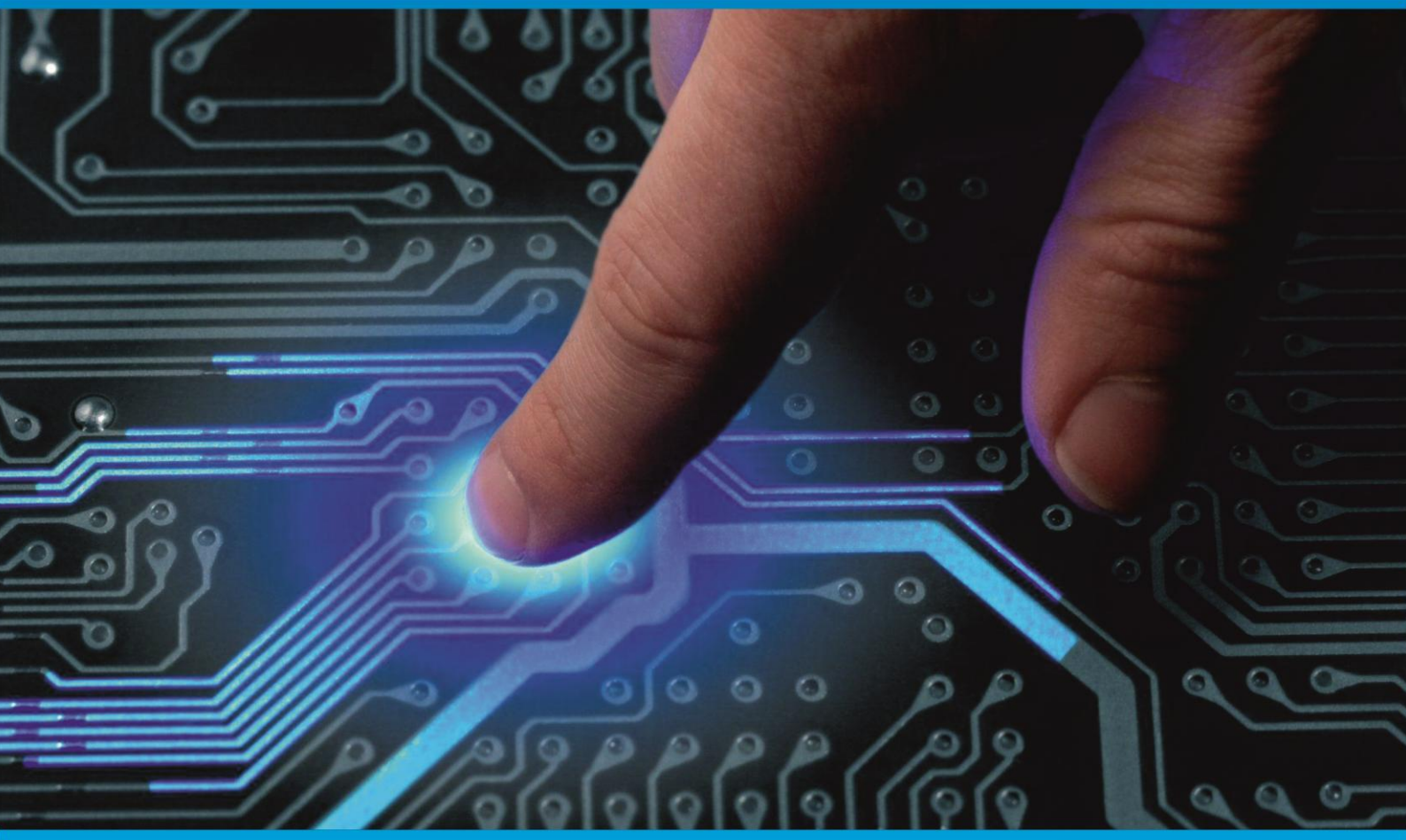
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 3, March 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.488

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 3, March 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0903047|

Smart Examination Hall Using Arduino

Sivaramakrishnan S, Sree Krishna B P, Hariharan S, Pranav S

UG Students, Dept. of ECE, Panimalar Engineering College, Chennai, India

ABSTRACT: Impersonation in exam halls is increasing day by day. This is due to careless and time-consuming traditional candidate checking and authentication system in exam halls. This project is designed to reduce impersonation in exam hall by verifying biometric features of the candidate. Each and every student will be issued an RFID card as their hall ticket and verifying that student in finger print. While they reaching the college premises and by showing their hall ticket to the RFID reader. Then verify the fingerprint to match the correct student. Our system consists of fingerprint scanner connected to arduino RFID data stored in database. The system is designed to pass only users by verifying their tag and fingerprint. The fingerprint system was designed to scan the fingerprint and ID numbers which were properly saved into the database of the system and confirm the eligibility of candidate for examination. It ensures only authorized users are allowed to enter the examination section and unauthorized users are not allowed to enter without any human intervention.

I. INTRODUCTION

1.1. RFID (Radio Frequency identification) technology is an emerging technology], used in a wide range of applications, is a member in the family of Automatic Identification and Data Capture (AIDC) technologies which is fast and reliable means for identification of objects. The RFID is composed of two main components. The Interrogator (RFID Reader) which transmits and receives the signal and the Transponder (tag) that is attached to the object. In an RFID system, RFID tags are "interrogated" by an RFID reader. The tag reader generates a radio frequency "interrogation" communicates with the tags. The reader also has a receiver that captures a reply signal from the tags and decodes that signal. The reply signal from the tags reflects, the tag's data content. The reply signal is created as passive "backscatter" An RFID tag is composed of a miniscule microchip and antenna. The RFID alone has numerous application but when is spliced with microcontroller the boundaries expands further.

1.2. Recognition of person based on biometric feature is an emerging phenomenon in our society. In the exam hall, authentication has always been a major challenge and verification of the authentic candidate is not an easy task and it consumes a lot of time and process. Traditional systems to verify a person's identity are based on knowledge (secret code) or possession (ID card), however codes can be forgotten or overheard and ID cards can be lost or stolen giving impostors the possibility to pass the identity test. The use of features inseparable form of person's body significantly decreases the possibility of fraud. Biometrics acts as a source for identifying a human being. This is used for authentication and identification purposes. In order to overcome the limitations of unimodal biometric system multimodal biometrics came into existence. It combines two or more biometric data recognition results such as a combination of a subject's fingerprint, palm and iris that increases the reliability of personal identification system that discriminates the approved and the fraudulent. Besides improving the accuracy, Multi-biometric systems are being progressively establish in many large-scale biometric applications because they have several advantages such as lower error rates and larger population coverage compared to uni-biometric systems. In this paper multimodal fusion of iris and palm vein images along with fingerprint sensor is proposed. Fingerprint based authentication is one of the beneficial biometric technique and are easily accessible, recognition requires minimal efforts on the part of the users, it does not capture information other than strictly necessary. Automated iris detection is yet another option for human identification and non-invasive verification. Interestingly, the spatial patterns of the human iris are highly distinctive to an individual. Among these, touch less palm vein authentication technology is integrated because of its high precision that comparing the vascular pattern under the skin, which are unique to each individual. The system is designed to pass only candidates validate by their biometric verification and block non-validate users.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 3, March 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0903047|

II. LITERATURE SURVEY

[1]. R.Tolosana, R. Vera-Rodriguez et al., s"Exploring recurrent neural networks for on-line handwritten signature biometrics," IEEE Access, pp.1– 11, 2018.

Systems based on deep neural networks have made a breakthrough in many different pattern recognition tasks. However, the use of these systems with traditional architectures seems not to work properly when the amount of training data is scarce. This is the case of the on-line signature verification task. In this paper, we propose a novel writer-independent on-line signature verification systems based on Recurrent Neural Networks (RNNs) with a Siamese architecture whose goal is to learn a dissimilarity metric from the pairs of signatures. To the best of our knowledge, this is the first time these recurrent Siamese networks are applied to the field of on-line signature verification, which provides our main motivation. We propose both Long Short-Term Memory (LSTM) and Gated Recurrent Unit (GRU) systems with a Siamese architecture. In addition, a bidirectional scheme (which is able to access both past and future context) is considered for both LSTMand GRU-based systems. An exhaustive analysis of the system performance and also the time consumed during the training process for each recurrent Siamese network is carried out in order to compare the advantages and disadvantages for practical applications. For the experimental work, we use the BiosecurID database comprised of 400 users who contributed a total of 11,200 signatures in four separated acquisition sessions. Results achieved using our proposed recurrent Siamese networks have outperformed the state-of-the-art on-line signature verification systems using the same database.

[2]. A.Toosi, A.Bottino, S.Cumani, P.Negri, and P. L. Sottile, "Feature fusion for fingerprint liveness detection: a comparative study,"IEEE Access, vol. 5, pp. 23 695–23 709, 2017.

Spoofing attacks carried out using artificial replicas are a severe threat for fingerprint-based biometric systems and, thus, require the development of effective countermeasures. One possible protection method is to implement software modules that analyze fingerprint images to tell live from fake samples. Most of the static software-based approaches in the literature are based on various image features, each with its own strengths, weaknesses, and discriminative power. Such features can be seen as different and often complementary views of the object in analysis, and their fusion is likely to improve the classification accuracy. This paper aims at assessing the potential of these feature fusion approaches in the area of fingerprint liveness detection by analyzing different features and different methods for their aggregation. Experiments on publicly available benchmarks show the effectiveness of feature fusion methods, which improve the accuracy of those based on individual features and are competitive with respect to the alternative methods, such as the ones based on convolutional neural networks.

[3]. D. Menotti, G. Chiachia et al.,"Deep representations for iris, face, and fingerprint spoofingdetection,"IEEE Trans. on Information Forensics and Security, vol. 10, no. 4, pp. 864–879, 2015.

Biometrics systems have significantly improved person identification and authentication, playing an important role in personal, national, and global security. However, these systems might be deceived (or spoofed) and, despite the recent advances in spoofing detection, current solutions often rely on domain knowledge, specific biometric reading systems, and attack types. We assume a very limited knowledge about biometric spoofing at the sensor to derive outstanding spoofing detection systems for iris, face, and fingerprint modalities based on two deep learning approaches. The first approach consists of learning suitable convolutional network architectures for each domain, whereas the second approach focuses on learning the weights of the network via back propagation. We consider nine biometric spoofing benchmarks - each one containing real and fake samples of a given biometric modality and attack type - and learn deep representations for each benchmark by combining and contrasting the two learning approaches. This strategy not only provides better comprehension of how these approaches interplay, but also creates systems that exceed the best known results in eight out of the nine benchmarks. The results strongly indicate that spoofing detection systems based on convolutional networks can be robust to attacks already known and possibly adapted, with little effort, to image-based attacks that are yet to come.

[4]. Naveen Raj, Avinash, Malaiyappan, "Examination Hall Guidance System Using Zigbee",Proceedings of AECE-IRAJ International Conference, Tirupati, India, ISBN: 978-81-927147-9-0, ,July 2013.

Students are facing difficulties for finding their examination rooms and their seats during the exams. our proposed methodology made a convenient solution for these difficulties. This paper, " ZIGBEE based Examination Hall Guidance System" presents a modernized method for examination hall management. our methodology overcomes

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 3, March 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0903047|

disadvantages of the existing system. Students are provided with LCD device controlled by Atmel microcontroller. ZIGBEE Transceiver attached with PC Database is made at the entrance of the building. Whenever the students enters the building, automatically communication happens through ZIGBEE and then students get the information about their seat allotment on their LCD display without getting any delay and no need of swiping the card.

[5]. Parvathy.A, Venkata Rohit Raj, Manikanta, Chaitanya.G, "RFID Based Exam Hall Maintenance System "IJCA Special Issue on Artificial Intelligence Techniques - Novel Approaches & Practical Applications AIT, 2011.

Seating Arrangement of students during examinations is distributed. Students face difficulties as they have to scrounge for their examination hall numbers and seating arrangement while they are wits end. An innovation which could aid the students in finding their exam halls and seats would be welcoming and very rewarding. This paper ―RFID BASED EXAM HALL MAINTENANCE SYSTEM‖, presents a modernized method of examination hall management. It is possible for a student to identify the particular exam hall from any other hall, when they swipe RFID card in a card reader located there. This helps them to identify the floor or get directions to their respective halls without delays. The card reader is provided at the entrance of the building, if the students enters wrongly a buzzer alarm sets off, otherwise the room number is displayed on the LCD, connected to controller.

III. EXISTING SYSTEM

This project proposes a solution for examinations based on jumbling system. It may cause students facing difficulty in finding their respective rooms. This system aids in finding respective exam halls and seats using RFID Technology. Each and every student is allotted an RFID Tag. Using RFID Technology, a valid candidate will be able to find his examination venue easily. The existing systems in which the authors implemented a model of secured and portable embedded reader system. Another existing system emphasis supply chain management which uses the application of RFID. Another review is the use of RFID in an integrated circuit to resolve inventory transactions issues.

DISADVANTAGE

- This system only having the RFID applications for examination venue.
- There is a possibility of fraud.

IV. PROPOSED SYSTEM

In our proposed system is to develop biometric based exam hall authentication systems that assist in the elimination of examination impersonation. Our system consists of a RFID and fingerprint sensor connected to arduino microcontroller circuit. In registration mode, the system allows to register up to 10 users and save their identity with respective id number. Then first verify the tag by using RFID reader and then verify the finger print of the student by using finger print scanner, if the both id will match means the student will allow inside the examination hall, if not means in the LCD display the unauthorized person will be displayed in the LCD and also send alert message by using GSM.

ADVANTAGES

- The identification based on biometric or fingerprint authentication is the efficient and reliable solution for stringent protection.
- This system is more accurate and faster than previous feature extraction finger print technology is expanding in real time applications of security measures since it is stable, secure and authentic.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 3, March 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0903047|

BLOCK DIAGRAM Power supply

HARDWARE REQUIREMENTS

- Power supply
  - Arduino uno
  - RFID reader and Tag
  - Finger print sensor
  - GSM
  - LCD

SOFTWARE REQUIREMENTS

- ARDUINO-IDE
- EMBEDDED C

VI. CONCLUSION

Seating Arrangement of students during examinations is distributed. Students face difficulties as they have to scrounge for their examination hall numbers and seating arrangement while they are wits end. An innovation which could aid the students in finding their exam halls and seats would be welcoming and very rewarding. This paper ―RFID BASED EXAM HALL MAINTENANCE SYSTEM‖, presents a modernized method of examination hall management. It is possible for a student to identify the particular exam hall from any other hall, when they swipe RFID card in a card reader located there. This helps them to identify the floor or get directions to their respective halls without delays. The card reader is provided at the entrance of the building, if the students enters wrongly a buzzer alarm sets off, otherwise the room number is displayed on the LCD, connected to controller.

REFERENCES

[1]. RubenTolosana, MartaGomez-Barrero, ChristophBusch, Javier Ortega-Garcia, Fellow, "Biometric Presentation Attack Detection: Beyond the Visible Spectrum", IEEE Transactions on Information Forensics and Security, 10.11.19/TIFS.2019.2934867.

[2].J. Galbally, S. Marcel, and J. Fierrez, "Biometric antispoofing methods: A survey in face recognition," IEEE Access, vol. 2, pp. 1530–1552, 2014.

[3].R.Tolosana, R. Vera-Rodriguez et al., s"Exploring recurrent neural networks for on-line handwritten signature biometrics," IEEE Access, pp.1– 11, 2018.

[4].A.Rattani, W.Scheirer, andA.Ross,"Opensetfingerprint spoof detection across novelfabricationmaterials,"IEEE Trans. on Information Forensics and Security, vol. 10, no. 11, pp. 2447–2460, 2015.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 3, March 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0903047|

[5]. D. Menotti, G. Chiachia et al.,"Deep representations for iris, face, and fingerprint spoofingdetection,"IEEE Trans. on Information Forensics and Security, vol. 10, no. 4, pp. 864–879, 2015.
[6].A. Toosi, A. Bottino, S. Cumani, P. Negri, and P. L. Sottile, "Feature fusion for fingerprint liveness detection: a comparative study,"IEEE Access, vol. 5, pp. 23 695–23 709, 2017.
[7].F. Nicolo and N. A. Schmid, "Long range cross-spectral face recognition: matching SWIR against visible light images,"IEEE Trans. on Information Forensics and Security, vol. 7, no. 6, pp. 1717–1726, 2012.
[8].A. Rattani and A. Ross, "Automatic adaptation of fingerprintliveness detector to new spoof materials,"in Proc. IEEE International Joint Conference on Biometrics, 2014, pp. 1–8.
[9].Maneesh Upmanyu, Anoop M. Namboodiri, Kannan Srinathan, and C. V. Jawahar, "Blind Authentication: A Secure Crypto-Biometric Verification Protocol," IEEE Transactions on Information forensics and security, vol. 5, no. 2, June 2010, pp.225-268.
[10].Ajay Kumar, Vivek Kanhangad, and David Zhang, "A New Framework for Adaptive Multimodal Biometrics Management,"IEEE Transactions on Information forensics and security, vol. 5, no. 1, March 2010p, p. 92-102.
[11].Abhishek Nagar, Karthik Nandakumar, Anil K. Jain, and Dekun Hu, "Multibiometric Cryptosystems Based on Feature-Level Fusion," IEEE Transactions on Information forensics and security, vol. 7, no. 1, February 2012, pp. 255–268.
[12].Koen Simoens, Julien Bringer, Herve Chabanne, and Stefaan Seys, " A Framework for Analyzing Template Security and Privacy in Biometric Authentication Systems," IEEE Transactions on Information forensics and security, vol. 7, no. 109 – 116 2, April 2012, pp. 833-841.
[13].Q. Zhang, Y. Yin, D. Zhan and J. Peng, "A Novel Serial Multimodal Biometrics Framework Based on Semisupervised Learning Techniques,"in IEEE Trans. on Info. Forensic and Sec., vol. 9, no. 10, pp. 1681-1694, Oct. 2014.
[14]. B. E. Manjunathswamy, J. Thriveni, andK.R.Venugopal, "Bimodal biometric verification mechanism using fingerprint and face images(BBVMFF),"inProc.IEEE 10th Int. Conf. Ind. Inf. Syst. (ICIIS), pp. 372-377, 2015.
[15].Y. Lin, E. Y. Du, Z. Zhou, and N. L. Thomas, "An efficient parallel approach for Sclera vein recognition," IEEE Trans. Inf. Forensics Security, vol. 9, no. 2, pp. 147–157, Feb. 2014.

INNO SPACE

SJIF Scientific Journal Impact Factor

Impact Factor:
7.488

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details