Gombe Journal of Geography and Environmental Studies (GOJGES)

Vol. 4 No.1 Jun. 2024
e-ISSN: 2714-321X
p-ISSN: 2714-3201

http://www.gojgesjournal.com

Addressing Error Rate Challenges in Biometrics for Building Automation

Ibrahim Hauwa Baba[1], Hussaini Lawal Musa [2], Muhammad Zainab Zakari[3]

[1]Building Department, School of Environmental Studies, Nuhu Bamalli Polytechnic, Zaria, Nigeria
[2] Building Department, School of Environmental Studies, Nuhu Bamalli Polytechnic, Zaria, Nigeria
[3]Department of Urban and Regional Planning, School of Environmental Studies, Nuhu Bamalli Polytechnic, Zaria, Nigeria.
Corresponding Authors Email: meijeeddah3@gmail.com, Tel: +234-8032873863.

Abstract

Biometric technology has revolutionised building automation by providing enhanced security and efficiency in access control systems, yet challenges persist, particularly with error rates such as False Acceptance Rate (FAR) and False Rejection Rate (FRR). These errors can significantly affect the reliability and effectiveness of biometric systems, especially in high-security environments. This study investigates the implementation of a fingerprint-based biometric system designed to minimize FAR and optimize FRR. The results showed that the system achieved a 0% FAR, meaning no unauthorized access was allowed, while the FRR was recorded at 5.7%, indicating that some legitimate users were wrongly denied access despite successful registration. The system's focus on security led to a trade-off, prioritizing the elimination of unauthorized access over minimizing false rejections. While achieving a 0% FAR is crucial for high-security environments like banks and prisons, the relatively high FRR highlights the need for system improvements to enhance user convenience. Several factors, including the quality of fingerprint samples (such as dirt or moisture) and environmental conditions, contributed to the FRR. To address these challenges, the study recommends adopting more advanced fingerprint sensors that can capture high-resolution images under various conditions, improving matching algorithms to handle slight variations in fingerprints, and integrating multi-modal biometrics, such as combining fingerprint recognition with iris or facial recognition, to reduce error rates. Additionally, regular updates and maintenance of biometric systems are essential to ensure they incorporate the latest technological advancements and maintain high accuracy over time

Keywords: Biometric Automation, Error Rates, Algorithm, Sensor, Building Automation

1.1 Introduction

Technological advancements have surpassed our expectations, bringing about innovations that significantly enhance security and efficiency in various fields. However, these advancements also pose challenges, particularly in security management. Biometric techniques have emerged as one of the most effective solutions for addressing these challenges. Although biometrics are not the sole component of automated identification systems, they offer a robust means of validation by providing a higher level of security, protection, and reliability in identification, access control, efficiency, and verification systems (Marcela, Ruben, & Jorge, 2021).

The application of biometrics in various structures, including schools, offices, hospitals, hotels, warehouses, and industries, is largely dependent on the required function. Despite their benefits, biometric systems face significant challenges, such as error rates and error bounds. Error bounds typically arise from sample size and correlation, while error

rates occur due to the system's acceptance or rejection of individuals. This paper aims to assess the error rates in biometric applications used in building construction automation. Error bounds are more closely related to factors such as sample resolution, system accuracy, speed, device size, and the occurrence of system errors (Mart, Brain, Ross, & Shahram, 2007).

Biometric systems encode bodily features to perform specific functions, with unique physical or behavioral characteristics serving as the basis for authentication (Nicholas, 2012). These systems analyze traits like fingerprints, palm prints, finger geometry, hand geometry, iris or retina patterns, facial recognition, voice comparison, signature dynamics, body odor, vein patterns, and typing rhythms. Given the effectiveness and versatility of these techniques, the quality and efficiency of biometric systems have become critical to their widespread adoption. Importantly, no viable alternative to biometrics in human identification for automation has been discovered to date (National Biometric Security, 2008).

Building automation combines control systems and computer networking to oversee and regulate security, power, lighting, HVAC, and other building operations (Johnson, 2014). Structures equipped with Building Automation Systems (BAS) are often referred to as "Intelligent Buildings," "Smart Buildings," or "Smart Homes" (KMC Controls, 2014). These systems enhance comfort and ensure optimal operational efficiency (Han et al., 2010). As such, minimizing error rates is essential when implementing biometric techniques in building automation.

In a rapidly advancing world, there is a growing need for research in this area to ensure that buildings are equipped with efficient and error-free automation systems, keeping pace with modern technological demands.

1.2 Determining the Efficiency of a Biometric System

The efficiency of a biometric system is evaluated using several key metrics, with the False Acceptance Rate (FAR) and False Rejection Rate (FRR) being the most critical.

- **False Acceptance Rate (FAR):** This represents the likelihood of the system incorrectly granting access to an unauthorized individual due to a mismatch between the biometric input and the stored template. FAR is typically expressed as a percentage, reflecting the proportion of invalid inputs that are wrongly accepted by the system (James, Issa & Isaac, 2016).

- **False Rejection Rate (FRR):** This metric indicates the probability of the system denying access to a legitimate user due to incorrect matching of the biometric input against the stored data. Like FAR, FRR is expressed as a percentage and represents the portion of valid inputs that are incorrectly rejected (James et al., 2016).

1.3 Review of Similar Works

A significant number of studies have been conducted on biometric systems for automated access control, exploring various approaches and technologies. One such example is the Contactless Palm Vein Biometrics System developed by Kah, which integrates both software and hardware for door access control. While this system provides a high level of security, it is hindered by the

inconvenience of positioning the hand correctly for scanning. Moreover, the device is mounted in public areas, leaving it vulnerable to vandalism and weather-related damage.

Fahmi's work on ear shape-based security door automation offers an alternative, where a smartphone camera is used to replace traditional biometric authentication. This system automatically unlocks a door when the user is in proximity to their home, utilizing location-based services (LBS) to authenticate the user via the smartphone's front camera, which captures the ear during a call. Although this method eliminates the need for a dedicated enrollment terminal and reduces costs, it is reliant on the proper functioning of the smartphone; any malfunction could result in a loss of access.

Mahdi developed a security door system regulated by "Time Zones" to enhance security in sensitive locations such as car parks, shopping centers, airports, or banks. The system automatically locks and unlocks doors based on predetermined time zones, offering an additional layer of security by managing access depending on the cardholder's authorization.

Falohun designed and implemented a biometrically controlled door system using iris recognition technology. His system also includes a power backup feature and relies on black iris data to simulate iris recognition algorithms in the prototype. This approach provides an advanced level of security, but the system's complexity could pose challenges for widespread implementation.

Merkow's contribution focuses on securing wireless communication using a finger chip module integrated with sensors. This standalone device includes a built-in CPU but is limited to systems using Bluetooth, restricting its application to specific communication environments.

Wang's project incorporates fingerprint and GSM technology to create a robust access control system. The system uses a high-voltage fingerprint scanner that operates in two modes: Master Mode for registering fingerprints and User Mode for regular access control. GSM commands allow the system to control its functions remotely, making it highly versatile and responsive to various inputs.

Lakshmi explored advancements in fingerprint identification by combining it with public key cryptography to enhance security. The fingerprint serves as a unique parameter for splitting the user's secret key, increasing the overall security of the system without needing to transmit authentication data during the process.

Ram and Gollapudi implemented a cost-effective locker security system using a combination of RFID, fingerprint, password, and GSM technologies. This standalone system compares mobile phone passwords with stored data to grant access. However, the reliance on passwords introduces potential vulnerabilities, as users may forget or misplace their credentials.

Sutar developed a high-security prototype for vehicle doors, which relies on a digitally authorized USB drive with encryption and decryption algorithms. While this system offers a two-step authentication process for enhanced security, it depends heavily on the owner's GSM, meaning access could be compromised if the GSM is lost or stolen.

Yugashini proposed an automatic door access system using face recognition and detection. By modifying principal

component analysis (PCA) into fast-based PCA (FBPCA), the system captures an image using a web camera and compares it to a database for authentication. If authenticated, the system opens the door or sends an SMS via GSM.

Okel designed a keyless door access system based on a smart card, controlled by a microcontroller unit. Similarly, Lay implemented a storage locker security system using fingerprint recognition to ensure that only the registered user could access their belongings. However, Lay's system requires a PC for operation, making it susceptible to data alteration.

Heraclius took a different approach by using stethoscopes and silicon NAM (Non-Audible Murmur) microphones to automate speech recognition systems. NAM microphones capture both audible and non-audible speech, offering privacy and noise resistance. The system integrates speech recognition into secure environments where confidentiality is critical.

2.1 Methods

The study focuses on both the software and hardware development of a biometric system where False Rejection Rate (FRR) records were specifically observed. A stratified random sampling method was adopted, ensuring that each member of the population had an equal chance of being selected. The biometric system was tested for its ability to either provide access through an electric lock or deny access when authentication failed. Secondary data for this study were sourced from literature reviews, including journals, conference papers, periodicals, and textbooks.

2.3 RESEARCH DESIGN

The system operates based on the four general stages of a biometric system namely: capture (This is the biometric registration process where a fingerprint is taken), extraction (This is an extracted biometric data of the fingerprint at the time of registration), comparism (This is when a fingerprint is compared with the existing data in the biometric system) and verification (This is for the system to verify that the finger print in contact is existing in the stored database of the system.

2.2 Biometric Enrolment Processes

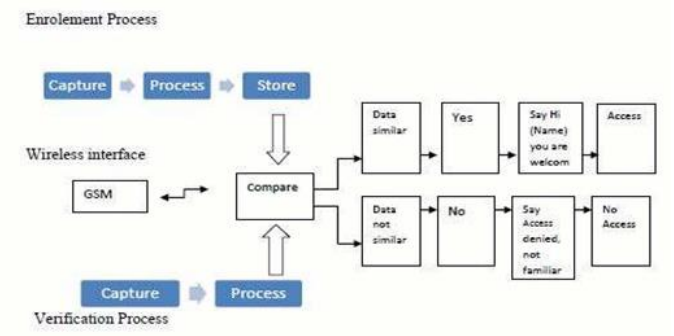

Figure 1. Enrolment process
Source: Field work (2017)

3.1 RESULTS AND DISCUSSION

3.1.1 Results

The Biometric automation system developed has no false acceptance (FAR), and only 4 False Rejection Rate (FRR), as can be observed below:

Table 1. The FAR and FRR error rates of the system

Items	Frequency	Percentage
Accessed	66	94.3%

Denied	4	5.7%
Total	70	100%

Source: Field work (2017)

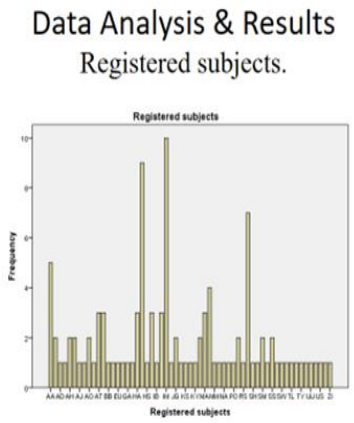

Figure 2: Registered subjects

The individual subjects registered were either on a single or double entry base. For single entries, the subjects only registered one finger, while the registration of between two to ten fingers is considered a double entry, as shown in figure 2 above.

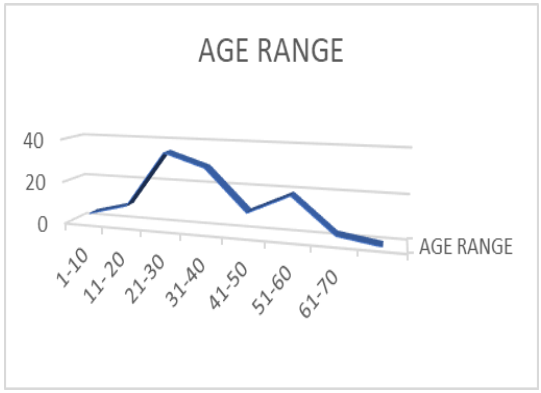

Figure 3: Age range of subjects

The registered subjects are predominantly in the 21 -30age range as observed in figure 3.2 above.

3.2.2 DISCUSSIONS

The designed biometric system does not allow access to a non- enrolled subject, even mistakenly (FAR=zero). However, the system denied access to four of the registered subjects, though their registration was successfully completed (FRR=4). Just as the efficiency of biometric systems are now improved, a system is usually designed to have either less FAR or FRR for better performance. Hence, for this research, the system has more FRR, which means the system would rather reject a

Registered subject than to allow access for an unregistered subject. Systems with higher FRR than FAR are used where security is highly desired like in banks, prisons, etc.

4. Conclusion

The basic errors in biometrics being: The False Acceptance Rate (FAR) and False Rejection Rate (FRR) errors, where monitored in a biometric system where fingerprint technology was adopted. The FAR was measured as 0%, while the FRR was measured as 5.7% In rare cases, some fingerprints may be rejected for enrolment due to various factors (i.e. dirt, dampness, flakes, etc.) and multiple enrolment by a single subject only recognises one of the finger prints in most cases.

REFERENCES

Adoghe, A.U. and I.A. Odigwe Adoghe. 2008. "Remote Monitor and Controller System for Power Generators". *Pacific Journal of Science and Technology*. 9(2):344-350.

Daugman, J. (2003), "The importance of being random: statistical principles of iris recognition", Pattern Recognition: 36(2): 279-291.

Daugman, J.(2004) , "How iris recognition works. IEEE on Circuits and Systems. For VideoTechnology 14: 1: pp 21–30.

Falohun, A. S. Omidiora, E.O. Fakolujo, O.A. Afolabi, O.A .Oke, A.O. Ajala, F.A. 2012. Development of a biometrically- controlled door system (using iris), with power backup. *American Journal of Sciences and Industrial Research*, AJSIRISSN:215349X,doi:10.5251/ajsir.2012.3.4.203.207, Pages 203-207.

Fahmi, A. P.N. Kodirov, E. Choi, A.D. and Lee, G. January, 2013. Hey Home, Open Your Door, I'm Back!Authentication System using Ear Biometrics for Smart Home. I*nternational Journal of Smart Home,Vol. 7,No.1.* Page 173-182.

Hamed, B. (2012). Efficient Authorized Access Security System Control Using ATMEL 89C55 & Mobile Bluetooth. *International Journal of Computer Theory and Engineering*, 4(1).

Han, K. Shon, T. and Kim,K. 2010. "Efficient mobile sensor authentication in smart home and WPAN", IEEE Trans. on Consum. Electron., vol. 56, no. 2.

Hawrra, H.A. & Al-Rubiae (2007). Design and Implementation of Computerized control room. *Journal of Karbala University,5*(2).Mahdi, S.A. 2013. *Development of Anti- Theft Door System for Security Room.* "Retrieved" 6th July 2014 "From" amam2012449@yahoo.com Savap International Natural and Applied Sciences: http.//www.Savap.org.pk.

Marcela H., Ruben M. and Jorge A. (2021). Biometric application in Education. *International journal on interactive design and manufacturing (JIDeM)15,365-380.*

Michael, M.G. Hoe,L.S. Connie,T.& Ket, C.(n.d.) *Contactless Palm Vein Biometrics System for Door Access.* "Retrieved" July 2014.

Mbamali, I. 2014. Lecture note *"Automatic Controls*" Building Services, Ahmadu Bello University Zaria.

Ping, W. Guichu, W.Wenbin, X. Jianguo, L. Peng,L. 2010. Remote monitoring intelligent system based on fingerprint door lock. *Intelligent computation Technology and automation (ICICTA), Vol.2.* 1012-1014.

Reyhani, S. and Mahdavi, M. 2007. "User Authentication Using Neural Network in Smart Home Networks", International Journal of Smart Home, vol. 1, no. 2, July, pp. 147-154.

Samuel, D. (2008). RFID security in door locks, Master thesis performed in information coding at Linköping Institute of Technology.

Vaidya, B. Park, J. H. Yeo, S. S. and Rodrigues, P. C.(2011) "Robust one-time password authentication scheme using smart card for home network environment", J Comp. Comm., vol.34, no. 3.

Wang, P. and Ku, C.C.2009. "A Variant-based Biometric Authentication Scheme Based on a Rotor Machine for Home Security", J. of Med. & Bio. Eng., vol. 29, no. 5.

Yakar M, Yılmaz H M and Mutluoglu O (2014). Performance of photogrammetric and terrestrial laser scanning methods in volume computing of excavation and filling areas. Arabian Journal for Science and Engineering, 39, 387-394. https://doi.org/10.1007/s13369-013-0