Quest Journals
Journal of Software Engineering and Simulation
Volume 10 ~ Issue 9 (2024) pp: 16-23
ISSN(Online) :2321-3795 ISSN (Print):2321-3809
www.questjournals.org

Research Paper

Design of Robotics Implementation of A Fingerprint Biometric System

Aremu Idris[1], Tiamiyu Olalekan[2], Ganiu Serifat[3], Davies Muyis[4], Olojede Mosebolatan[5]

[1] (*Department of Computer Science Lagos State University of Science and Technology, Lagos Nigeria)*
[2](*Department of Curriculum Teaching and Learning Studies Memorial University, Newfound Land Canada)*
[3](*Department of Computer Science Western Governor University, Utah USA)*
[4](*Department of General Studies Lagos State University of Science and Technology, Lagos Nigeria)*
Corresponding author: Tiamiyu Olalekan e-mail: tiadgreat@gmail.com

ABSTRACT : *Biometrics, rooted in the Greek terms "bios" (life) and "metrikos" (measure), represents a modern approach to identifying individuals based on their unique physical characteristics, such as fingerprints, facial features, and iris patterns. In today's increasingly digital landscape, traditional security methods like passwords and keys have become inadequate in safeguarding sensitive information. The rise of sophisticated cyberattacks and unauthorized access has highlighted the need for more advanced and secure authentication methods. This project aims to design and implement a fingerprint biometric system using robotics and FPGA technology. The system is intended to provide a more reliable and secure method of verifying identities by capturing and processing fingerprint images. It will extract minutiae points, the unique features within a fingerprint, to create a robust authentication mechanism. This approach promises to enhance security by offering an alternative to conventional methods that are often vulnerable to breaches. In developing this biometric system, the focus will be on ensuring that it can be effectively integrated into various applications where secure access control is crucial. By leveraging the unique and immutable nature of fingerprints, the system will reduce the risks associated with password reuse, theft, and unauthorized sharing. The inclusion of continuous authentication techniques will further strengthen security, ensuring that the user's identity is verified throughout a session, not just at the initial login. Additionally, the project will incorporate version control mechanisms to track the development and deployment of the system, ensuring that any changes or updates can be easily managed and reviewed. This will help maintain the system's reliability and effectiveness over time, allowing it to adapt to evolving security challenges. Through this work, we aim to contribute to the broader adoption of biometric technologies in securing digital and physical environments, paving the way for more secure and seamless user experiences.*

KEYWORDS*: Biometrics, fingerprints, authentication, digital, physical environments, security*

R*eceived 03 Sep., 2024;* ***R****evised 14 Sep., 2024;* ***A****ccepted 16 Sep., 2024 © The author(s) 2024.*
P*ublished with open access at* ***www.questjournas.org***

I. INTRODUCTION

1.1 Background

The word "biometric" comes from the Greek words "bios" (life) and "metrikos" (measure), representing the measurement of life. Biometrics involves using unique physical traits, like fingerprints, facial features, or iris patterns, to identify and verify someone's identity [1]. This method has become essential in modern security, offering a more secure way to access facilities, networks, or computers compared to traditional methods like passwords or keys [2]. The power of biometric authentication lies in its ability to provide a level of security that is difficult to bypass, making it a key element in protecting sensitive information.

Biometrics, or biometry, is the science of analyzing human characteristics through mathematical and statistical methods. This field has found significant applications in security, from accessing computers remotely to controlling entry into physical locations and authorizing transactions [3]. What makes biometric recognition

stand out is its reliability—unlike passwords or ID cards, biometric traits can't be easily shared, forgotten, or copied. Commonly used traits include fingerprints, facial recognition, iris patterns, and voice, all of which are now widely used in commercial systems.

Fingerprint identification, one of the oldest and most trusted biometric methods, plays a crucial role in security. Every fingerprint is unique, formed by ridges and furrows on the skin, with specific points called minutiae that make each print distinctive. These minutiae points are the key to comparing fingerprints and ensuring accurate identification. Research shows that it's extremely unlikely for two individuals to share even eight common minutiae points, making fingerprint-based systems both reliable and secure [4].

As biometrics continues to evolve, integrating it with artificial intelligence (AI) is becoming a focus. The aim is to develop systems that can learn from users and adapt to them, making the authentication process smoother and more intuitive. With biometric technology becoming more widespread, the need for physical keys, cards, or fobs might soon disappear, leading to a future where identity verification is seamless and secure. Continuous authentication (CA) takes this a step further by ensuring that a user's identity is verified throughout their entire session, not just at the start, adding an extra layer of security against potential threats [5].

1.2 Statement of Problem

As our world becomes more digital, keeping sensitive information secure is getting harder. Traditional security methods like passwords and keys, once considered enough, are now vulnerable to increasingly sophisticated cyberattacks and unauthorized access [6]. With the rise of digital devices and online services, there's a growing need for stronger security measures. A big problem with passwords is that people often reuse them across different platforms, which makes them easy targets for hackers. Moreover, passwords can be lost, stolen, or shared, putting systems and data at risk.

1.3 Aims and Objectives

This project aims to design and build a fingerprint biometric system using robotics and FPGA technology to create a more secure ways of verifying identities. The system will focus on capturing and processing fingerprint images, extracting key features to ensure accurate identification. The specific objectives are to:

1. Review existing research and literature on fingerprint biometric systems.
2. Design and develop a system that can process fingerprint images and extract minutiae points, which are crucial for accurate identification.
3. Implement this system on an embedded processor using an FPGA development board.
4. Create a version control system to track changes and revisions, allowing users to access and revert to previous versions when needed.

By achieving these objectives, the project hopes to offer a more secure and reliable alternative to traditional authentication methods, helping to protect both digital and physical spaces from unauthorized access.

II. Literature Review

The proposed system introduces fingerprint authentication into the attendance management process, aimed at both employees and enterprises [7]. The process involves two primary steps: enrollment and authentication. During enrollment, a user's fingerprint is captured, and specific features are extracted and stored in a database as a template, alongside the user's ID. This template serves as a reference for future authentication, where the user's fingerprint is again captured and compared to the stored template. If the fingerprints match, the system logs the attendance under the corresponding user ID. The system utilizes a fingerprint reader for capturing images, coupled with software that processes the fingerprints and a database that stores user information, including attendance records [8].

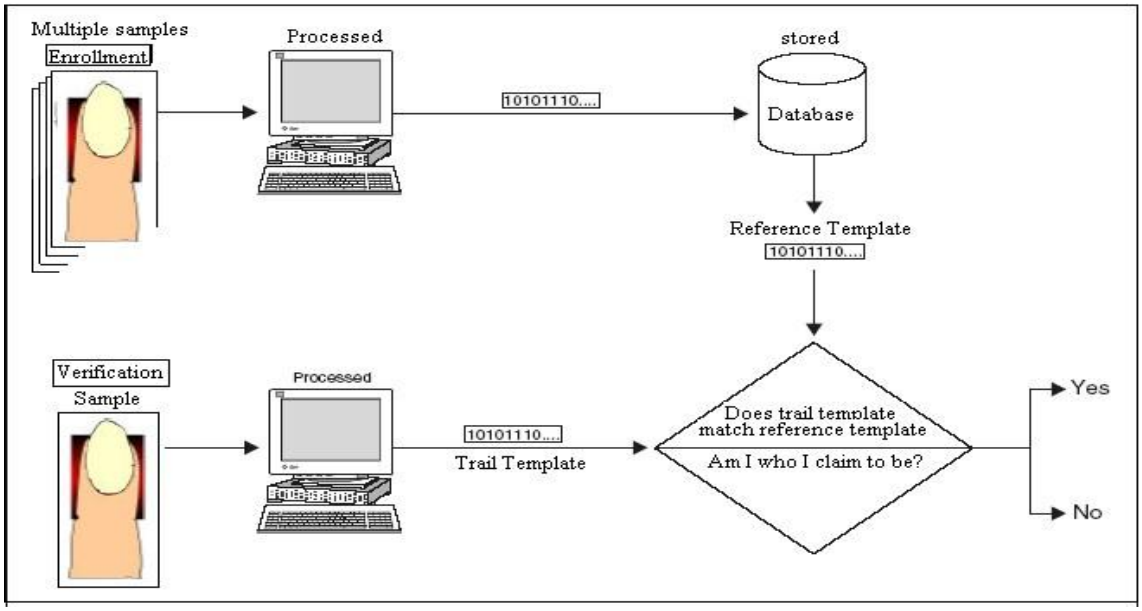

Figure 2.1 Architecture of the proposed attendance management system.

2.1 System Architecture

The architecture of the system is divided into three main stages: Enrollment, Authentication, and System Database [9]. In the Enrollment stage, users are registered into the system by capturing their fingerprints and other personal information, which is stored as a template in the database. This process includes capturing two samples of each fingerprint to ensure quality and accuracy. The Authentication stage involves comparing the live fingerprint with the stored template during each attempt to access the system [10]. The System Database manages all stored data, including user bio-data and attendance records. This structure ensures a secure and efficient system for managing attendance.

2.2 Fingerprint Recognition

Fingerprint recognition relies on the unique patterns of ridges and minutiae points on an individual's finger. This method is highly accurate and widely used for identification and verification, as it distinguishes between different individuals' fingerprints. The recognition process includes enrollment (capturing and storing fingerprints), verification (comparing a live fingerprint with the stored template), and identification (determining the identity of a person based on their fingerprint).

2.3 Overview of Access Control Management

The proposed system integrates fingerprint authentication with access control management, particularly for managing attendance. During enrollment, a user's biometric data, including fingerprint minutiae, is captured and stored in a database [11]. For authentication, the user's fingerprint is again captured and compared to the stored data to verify their identity. This process is managed by an administrator who oversees both the enrollment and authentication stages, ensuring that attendance records are accurately maintained.

2.4 Review of Related Work

Several studies have explored various biometric authentication methods, including fingerprint recognition. For instance, Shoewu [12] proposed an embedded computer-based system for attendance management using electronic cards and readers. However, this method relies heavily on physical cards, which can be lost or tampered with. Other studies have explored facial recognition algorithms for access control, though these can be less reliable due to changes in a person's appearance over time [13]. While there are studies that specifically concentrates on the most recent databases, 2D and 3D face recognition methods [14]. Besides, it pays particular attention to deep learning approach as it presents the actuality in this field [15]. Fingerprint-based systems, by contrast, offer a higher level of accuracy and security, making them more suitable for robust access control and attendance management systems.

Table 2.0 Comparison of various biometric Technologies

Biometric characteristic	Universality	Distinctiveness	Permanence	Collectability	Performance	Acceptability	Circumvention
Facial thermogram	H	H	L	H	M	H	L
Hand vein	M	M	M	M	M	M	L
Gait	M	L	L	H	L	H	M
Keystroke	L	L	L	M	L	M	M
Odor	H	H	H	L	L	M	L
Ear	M	M	H	M	M	H	M
Hand geometry	M	M	M	H	M	M	M
Fingerprint	M	H	H	M	H	M	M
Face	H	L	M	H	L	H	H
Retina	H	H	M	L	H	L	L
Iris	H	H	H	M	H	L	L
Palmprint	M	H	H	M	H	M	M
Voice	M	L	L	M	L	H	H
Signature	L	L	L	H	L	H	H
DNA	H	H	H	L	H	L	L

III. METHODOLOGY

3.1 Approach

The proposed automated fingerprint Biometric system conceptualized in below comprises the following phases:

a) Fingerprint Acquisition/ Enrollment
b) Fingerprint Image Enhancement
c) Minutiae Extraction
d) Minutiae Matching
e) Fingerprint Classification/Authentication

3.2 Fingerprint Acquisition

The proposed method for this thesis is the live scan/on-line method because it is fast and easy to use without necessary need for expertise unlike the offline method, which is cumbersome, slow and returns large deformations due to the inherent nature of the rolled acquisition process despite the need for practice and skill for its use.

3.3 Fingerprint Sensing

There are two primary methods of sensing/acquiring a fingerprint image:

(a) **Inked scan (off-line):** The off-line approach is used to produce an impression of the finger on an intermediate medium such as paper.

(b) **Live scan (ink-less or on-line):** The live-scan fingerprint is a collective term for a fingerprint image obtained directly from the finger without the intermediate step of getting an impression on paper.

3.4 Fingerprint Storage

The features extracted during enrolment are saved in a formulated fingerprint database as fingerprint template (in binary format) for future comparison against other fingerprint templates. The database stores the fingerprints and other unique information of each and every fingerprint. For each fingerprint, the following information is stored in the database [16]:

a. An identification number associated to the person whose fingerprint was captured
b. The fingerprint templates
c. The fingerprint owner's name

Using the available information in the database, the following tasks could be performed:
Form an association between the fingerprint and the owner. Associate extracted features to a particular fingerprint.

3.5 Fingerprint Classification

Fingerprint classification identifies the common overall patterns in fingerprints. Global representations include locations of critical points (e.g., core and delta) in a fingerprint. A typical fingerprint classification scheme categorizes the prints into the following six major classes: whorl, right loop, left loop, arch, twin loop, and tented arch. Sometimes, a synthetic category called scars is included to classify fingerprints mutilated with scars, thus obscuring the possibility of accurately determining its true class. It is at this stage that the minutiae set obtained from an individual's fingerprint is stored as a template for that subject. When analyzed at the global level, the fingerprint pattern exhibits one or more regions where the ridge lines assume distinctive shapes (characterized by high curvature, frequent termination, etc.) [17]. These regions (called singularities or singular regions) may be classified into three typologies: loop, delta, and whorl. Singular regions belonging to loop, delta, and whorl types are typically characterized by ∩, Δ, and O shapes respectively [18].

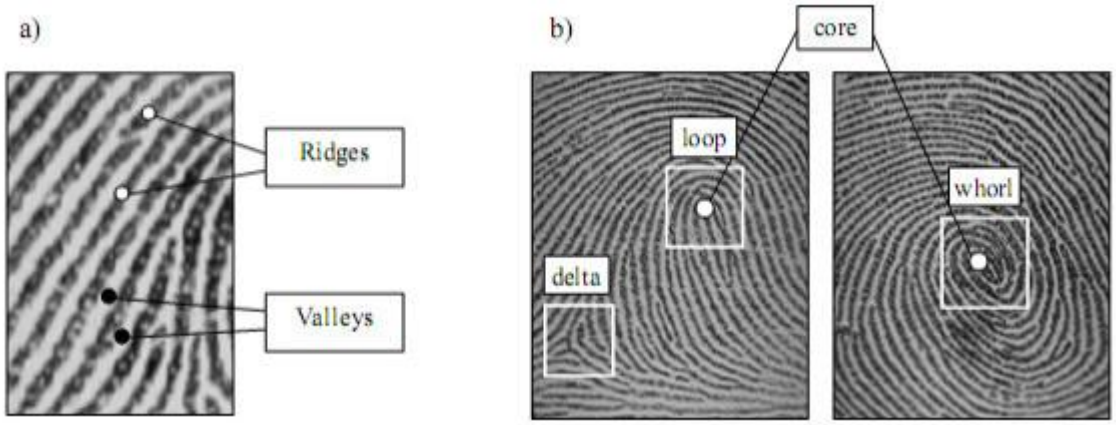

Figure 3.1 a) Ridges and valleys on a fingerprint image;b) singular regions (white boxes) and core points (small circles) in fingerprint images.

3.6 Minutiae Extraction

Minutiae extraction is a process of studying and deriving useful information from filtered image
Patterns [18]. The derived information may be general features which are evaluated to ease further processing. For example, in image recognition, the extracted features will contain information about gray shade, texture, shape or context of the image. This is the main information used in image processing.
Extracting minutiae from the skeleton of the fingerprint requires a method that is able to distinguish and categorize the different shapes and types of minutiae [19,20]. At this stage of the proposed algorithm, the Crossing Number (CN) method will be employed. This concept would be adopted with the use of the skeleton image where the ridge flow pattern is eight connected.

The following are the major tasks that would form this stage:
a) Minutiae extraction by scanning the local neighborhood of each ridge pixel in the image using a 3x3 window.
b) Computation of CN value, which is defined as half the sum of the differences between pairs of adjacent pixels in the eight neighborhood.
c) Classification of the ridge properties into ridge ending, bifurcation or non-minutiae point. Identification of ridge pixel with three-ridge pixel neighbors as ridge bifurcations and those with one ridge pixel neighbors as ridge endings.
The CN for a ridge pixel *P* is given by

$$CN = 0.5 \sum_{i-1}^{8} |P_i - P_{i+1}| \quad P_9 = P_1$$

where *Pi* is the pixel value about *P*. For a pixel *P*, its eight neighboring pixels are scanned into an anti-clockwise direction.

3.7 Feature Matching

The extracted unique details from the fingerprint come together to form a point pattern in plane. Therefore, matching two minutiae point patterns with each other is considered a 2-D point pattern problem. Hence, an algorithm that localizes the maximum number of mutual points in the two-point patterns is adopted for this research. A minutia is determined by its attributes. Matching the minutia is to match its three attributes. In this algorithm, noting that the three attributes are independent and do not overlap, we can separately calculate the possibility of matching one attribute. After casting grids on two fingerprints, namely A and B, only the "effective area" is considered as shown below.

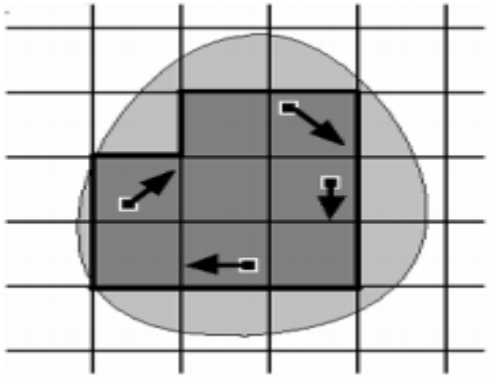

Figure 3.2 Grids on a fingerprint

3.8 Distribution Fitting Side length of grid r:

In an actual fingerprint image, the value of M is related with r - the side length of the grids. r should be so large that the same minutia point in different images can fall in the same grid, meanwhile r should be small enough to contain at most one distinct minutia. So, the value of r should be determined with great caution. The approach here is to fit the distribution of position distance of the same minutia in different impressions along x and y axes separately, from which we can choose a proper lower bound of r.

This algorithm involves the following:
a. Detection of a minutia by its attributes.
b. Matching the 3 attributes (number, direction and type/class) of each minutia.

i) Matching in grid number
ii) Matching in direction
iii) Matching in type
iv) Matching of minutiae
Considering the assumption that the three attributes are independent, the probability that two minutiae are matched in both direction and type is obtained from the product of the two separate probabilities.

IV. IMPLEMENTATION AND RESULT

The system is built using Java for the front-end and MySQL as the back-end database, running on a Windows operating system. The design follows four main steps:

1. Initialize the Fingerprint System Library
2. Capture Fingerprint Images
3. Extract Templates
4. Enroll or Match Templates

The fingerprint reader triggers specific events for capturing, processing, and storing images. If the image quality is insufficient, the system prompts for a fresh capture until a satisfactory image is obtained, ensuring accurate enrollment.

4.1 Fingerprint Application

To ensure high-quality fingerprint captures, the system requires firm pressure when placing the finger on the scanner. The system assesses the image quality before allowing enrollment, preventing errors and duplicate

entries. After enrollment, the system can automatically identify a fingerprint when scanned, displaying the owner's details to avoid duplicates.

4.2 Fingerprint Database

Captured fingerprints are stored in a MySQL database, serving as the system's back-end.

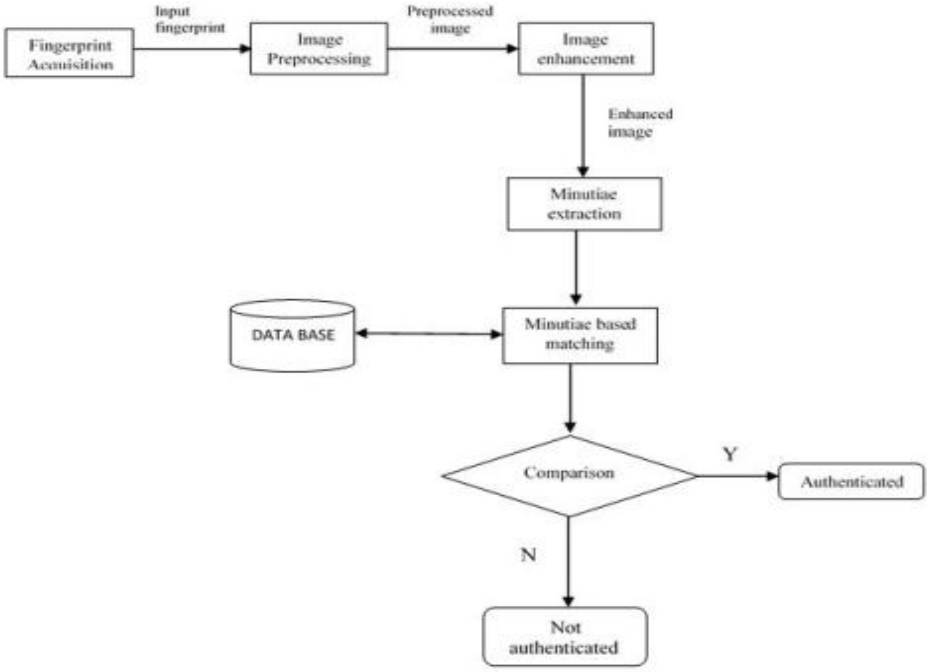

Figure 4.1 Fingerprint Recognition System

4.3 System Performance Analysis

The system's accuracy is measured by the False Acceptance Ratio (FAR) and False Rejection Ratio (FRR). With a 1% FAR and a 7% FRR, the system achieves a 95% accuracy rate. Proper finger pressure is crucial for accurate captures, and regular cleaning of the scanner is recommended to avoid errors.

Rate	Percentage
False Acceptance Ratio (FAR)	1%
False Rejection Ratio (FRR)	7%
Accuracy	95%

Table 4.1 System Performance Analysis

4.4 System Testing

The system underwent several testing phases to ensure reliability:

1. Unit Testing: Individual components were tested for functionality.
2. Integration Testing: Tested how well different components worked together.
3. Acceptance Testing: Ensured the system met user requirements and quality standards after implementation.

V. CONCLUSION AND RECOMMENDATIONS

5.1. Summary

This project aimed to create a system for collecting attendance. With issues of trust, credibility, and user apathy recurring in the traditional manual method of taking attendance with the access controlling community, the development of this attendance system with fingerprint biometrics authentication - specifically the use of access control will be a welcome innovation to the attendance process in general. This project implements a biometric attendance system for enterprise in order to reduce, if not eliminate, the issues of eligibility, erroneous user information, and the centralized and stressful human attendance routine.

5.2. Conclusion

The critical factor for the pervasive utilization of fingerprints is in meeting the key performance metrics (such as matching speed and accuracy) standards demanded by emerging civilian identification applications. Unlike an identification based on passwords or tokens, performance of the fingerprint-based identification is not perfect. There will be a growing demand for faster and more accurate fingerprint matching algorithms which can (particularly) handle poor quality images. Some of the emerging applications (e.g., fingerprint-based smartcards) will also benefit from a compact representation of a fingerprint. The design of highly reliable, accurate, and foolproof biometrics-based identification systems may warrant effective integration of discriminatory information contained in several different biometrics and/or technologies. The issues involved in integrating fingerprint-based identification with other biometric or non-biometric technologies may also constitute another important research topic.

5.3. Recommendation

The following recommendations of this system implementation may simplify and ease the burden for the administrators as reporting and analyzing of data will be improved. Several improvements can be done for further development as follow:

i. Upgrade to mobile application: Mobile application will be more practical since the emergence of mobile application technology has become a bridge to communication and expand profit in more business industries.

ii. Reporting: More related reports should be produced to see more information about the users.

REFERENCES

[1]. Perwej, Y. (2023). An Empirical Investigation of Human Identity Verification Methods. International Journal of Scientific Research in Science, Engineering and Technology, 10(1), Pages-16.

[2]. Hassan, W., Chou, T. S., Li, X., Appiah-Kubi, P., & Tamer, O. (2019). Latest trends, challenges and solutions in security in the era of cloud computing and software defined networks. Int J Inf & Commun Technol ISSN, 2252(8776), 8776.

[3]. Alrawili, R., AlQahtani, A. A. v;nS., & Khan, M. K. (2024). Comprehensive survey: Biometric user authentication application, evaluation, and discussion. Computers and Electrical Engineering, 119, 109485.

[4]. Mondal, A. (2021). An Overview Of Latent Fingerprint Matching. Webology (ISSN: 1735-188X), 18(3).

[5]. Olanrewaju, R. F., Khan, B. U. I., Morshidi, M. A., Anwar, F., & Kiah, M. L. B. M. (2021). A frictionless and secure user authentication in web-based premium applications. Ieee Access, 9, 129240-129255.

[6]. Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. Electronics, 12(6), 1333.

[7]. Ali, N. S., Alhilali, A. H., Rjeib, H. D., Alsharqi, H., & Al-Sadawi, B. (2022). Automated attendance management systems: systematic literature review. International Journal of Technology Enhanced Learning, 14(1), 37-65.

[8]. PAUL, G. (2022). FINGERPRINT BIOMETRICS ATTENDANCE SYSTEM USING MOUNTAIN TOP UNIVERSITY AS A CASE STUDY.

[9]. Sarkar, A., & Singh, B. K. (2020). A review on performance, security and various biometric template protection schemes for biometric authentication systems. Multimedia Tools and Applications, 79(37), 27721-27776.

[10]. Sarkar, A., & Singh, B. K. (2020). A review on performance, security and various biometric template protection schemes for biometric authentication systems. Multimedia Tools and Applications, 79(37), 27721-27776.

[11]. Joshi, M., Mazumdar, B., & Dey, S. (2020). A comprehensive security analysis of match-in-database fingerprint biometric system. Pattern Recognition Letters, 138, 247-266.

[12]. Shoewu, O. O., Akinyemi, L. A., Lawal, R. A., & Otagburuagu, O. R. (2020). Enhanced Smart Biometric Based Attendance (ES2BASYS) System Interfaced with POS Facility for a Smart Academic Institution. The Pacific Journal of Science and Technology, 21(2), 59-70.

[13]. Adjabi, I., Ouahabi, A., Benzaoui, A., & Taleb-Ahmed, A. (2020). Past, present, and future of face recognition: A review. Electronics, 9(8), 1188.

[14]. Adjabi, I., Ouahabi, A., Benzaoui, A., & Taleb-Ahmed, A. (2020). Past, present, and future of face recognition: A review. Electronics, 9(8), 1188.

[15]. Wang, X., Han, Y., Leung, V. C., Niyato, D., Yan, X., & Chen, X. (2020). Convergence of edge computing and deep learning: A comprehensive survey. IEEE Communications Surveys & Tutorials, 22(2), 869-904.

[16]. Delac, K., & Grgic, M. (2004, June). A survey of biometric recognition methods. In Proceedings. Elmar-2004. 46th International Symposium on Electronics in Marine (pp. 184-193). IEEE.

[17]. Bouguerra, M. (2022). Fingerprint Recognition and Classification (Doctoral dissertation, Larbi Tebessi University-Tebessa).

[18]. Maltoni, D., Maio, D., Jain, A. K., & Feng, J. (2022). Fingerprint analysis and representation. In Handbook of fingerprint recognition (pp. 115-216). Cham: Springer International Publishing.

[19]. Nirmalakumari, K., Rajaguru, H., & Rajkumar, P. (2019, April). Efficient minutiae matching algorithm for fingerprint recognition. In 2019 International Conference on Advances in Computing and Communication Engineering (ICACCE) (pp. 1-5). IEEE.

[20]. Maio, D., & Maltoni, D. (2022). Minutiae extraction and filtering from gray-scale images. Intelligent biometric techniques in fingerprint and face recognition, 153-192.

[21]. Valdes-Ramirez, D., Medina-Pérez, M. A., Monroy, R., Loyola-González, O., Rodríguez-Ruiz, J., Morales, A., & Herrera, F. (2019). A Review of Fingerprint Feature Representations and Their Applications for Latent Fingerprint Identification: Trends and Evaluation. IEEE Access, 7(1), 48484-48499.

[22]. Krish, R. P., Fierrez, J., Ramos, D., Alonso-Fernandez, F., & Bigun, J. (2019). Improving automated latent fingerprint identification using extended minutia types. Information Fusion, 50, 9-19.