Biometric Fingerprint Authentication of South African Banks

NDOU.R
222841577
Tshwane University of Technology
Computer Systems Engineering
Soshanguve,South Africa

TLOOME C.C
221187601
Tshwane Universsity of Technology
Computer SystemsEngineering
Soshanguve,South Africa

MOGANO P.P
220551822
Tshwane University of Technology
Computer Systems Engineering
Soshanguve,South Africa

Abstract - ***In our project, we created a cutting-edge fingerprint recognition system designed specially for banks in South Africa. Our main objective was to strengthen security measures in financial institutions, addressing concerns about illegal access and the protection of consumer data. We were able to do this thanks to the use of sophisticated fingerprint recognition technology, which greatly lowers the chances of identity theft and fraudulent transactions.***

Our strategy involves fusing sophisticated hardware elements with fingerprint recognition algorithms. We used Quartus software for effective FPGA implementation. Our system successfully identifies and authenticates users by utilizing the distinctive fingerprint patterns of each user. The robust FPGA design capabilities of Quartus platform were crucial to the success of our project and allowed us to develop a reliable and effective solution for South African banks.

By using the biometric security system, South African banks might modernize their security procedures and provide a high degree of protection for both their clients and their financial institutions. This project increases confidence and trust among bank clients while simultaneously enhancing security. Quartus provided reliable hardware acceleration, and also provided a versatile framework for smooth system integration, both of which were essential components of our project.

Keywords - Finite State Machine, Fingerprint Recognition Algorithm, Biometric Security System.

I. INTRODUCTION (*HEADING 1*)

The incorporation of cutting-edge technologies has had a significant impact on our lives in today's world of rapid evolution, notably in the area of security systems. The landscape of security measures has changed due to the introduction of new technologies and creative detection techniques, which have improved their effectiveness, dependability, and responsiveness to the ever-increasing threats posed by unauthorized access and data breaches. Biometric authentication has gained popularity in the security sector in recent years. Banks in South Africa have added biometric authentication systems to their security measures. Examples are, Biometric identification and verification systems have been installed at Absa and FNB's branches [2]. Capitec Bank has implemented biometrics to boost client transaction security and reduce banking fees [4]. To enable banks to conduct online fingerprint verification of their clients, the South African Banking Risk Information Centre (SABRIC) and the Department of Home Affairs (DHA) have signed a project agreement [4]. Mastercard has introduced a biometric card that authorizes in-store purchases using the cardholder's fingerprint rather than a PIN or signature [1]. These biometric authentication technologies have been proven to be successful in enhancing bank card transaction security protocols [4].

Banks in South Africa have fingerprint-based biometric authentication systems in place to strengthen their security measures. Similar security-related initiatives include Thales' development of facial recognition technology for use in government security initiatives like locating missing children [7] [8]. Additionally, Thales provides solutions for a range of uses, including border control and law enforcement [8]. The National Institute of Justice performed study on how technology will affect 21st-century policing tactics [9]. A manual on user access security, which covers password maintenance and selection, was issued by the National Center for Education Statistics [10]. Identity and access management programs gain an additional degree of security thanks to two-factor authentication [11]. These initiatives show the range of uses for security recognition technology as well as the value of stakeholder input throughout implementation [12].

We carefully selected fingerprint recognition as the cornerstone of our biometric identification system because of its unrivaled uniqueness and stability, which have been verified by studies from Jain et al. (2016) and Maltoni et al. (2009) [13] [14]. My objective of increasing the security of bank card transactions is well aligned with fingerprint recognition because it provides a non-intrusive, user-friendly, and quick authentication mechanism. As shown by Patel et al. (2015), integrating finite state machines and multiplexers into our hardware architecture guarantees effective processing and precise fingerprint data matching,

ensuring the security of financial transactions while boosting user experience [15]. This strategy combines state-of-the-art technology with tried-and-true methods of hardware design, offering strong security and quick, efficient authentication procedures inside a small framework.

Our biometric authentication solution brings transformational benefits to South African banks. Improved security fortifies customer accounts, preventing unauthorized access and fraud, in line with the success of Absa, FNB, Capitec, and others [16], [17]. The system optimises user experience by replacing manual methods with smooth fingerprint recognition, significantly reducing transaction times and improving customer satisfaction. In line with industry trends such as SABRIC, Mastercard, and others, it ensures the banks' competitiveness and technological excellence. Reduce fees, build trust, and foster loyalty. This system strengthens long term customer relationships, improving the institutions' reputations. Positioned as leaders in the industry, South African Banks demonstrate their commitment to security, setting new benchmarks and ensuring their relevance in a digital era.

The last paragraph now is about the organization of the Report : (Leave it as it is as I am writing it for you) : The remainder of this report is organized as follow: Section two discuss the background and related work on " Fill in the name of your project". Section 3 shown the methods used for this project. Section 4: Shows the simulation obtained while section 5 discuss the obtained results. Finally section 6 conclude the report.

II. BACKGROUND : RELATED WORK

In the modern society scene, our biometric authentication solution stands out as a beacon of innovation and security. Our idea solves a vital need for financial institution security by seamlessly merging cutting-edge fingerprint recognition technology with efficient hardware design. In an era of digital transactions and increasing cybersecurity risks, the impact of our system is substantial. It not only transforms banking security but also sets new standards for user experience. Our project changes the way individuals engage with banking services by providing a secure, quick, and user-friendly authentication method. This transition, based on modern biometric technology, not only improves security but also instill trust, producing a digital environment in which individuals may have confidence in the security of their financial transactions.

1. Touch ID and Face ID technology from Apple:
My biometric authentication technology is closely related to Apple's Touch ID and Face ID technologies. They, like my project, use biometric data (fingerprint and facial recognition, respectively) to improve user security. These technologies have proven critical in mobile device security, allowing seamless and secure access to smartphones and tablets. These technologies are significant because of their widespread acceptance and impact on user convenience and security. Similarly, my biometric authentication solution strives to improve banking security by enabling safe and user-friendly access to financial services. My concept coincides with the trend of incorporating biometric authentication into daily technology, delivering robust security and user delight by leveraging the success of Touch ID and Face ID.

2. The Samsung Pass:
Samsung Pass is a biometric authentication system that allows users to log into websites and apps using biometric technologies such as fingerprint recognition. In terms of using fingerprint recognition for identification, this effort is identical to mine. Samsung Pass is noteworthy because it extends biometric security beyond device access, providing customers with a safe way to authenticate themselves across many platforms. Similarly, my initiative focuses on using fingerprint recognition to secure financial transactions in the banking sector. My study stresses the need of extending biometric security solutions to vital areas such as banking, providing secure and efficient digital interactions for customers by drawing parallels with Samsung Pass.

3. Biometric Card Technology from MasterCard:
Biometric card technology from Mastercard integrates fingerprint recognition directly into credit and debit cards, allowing customers to authorize transactions with their fingerprints. In terms of using fingerprint recognition for transaction authorization, this approach is similar to mine. Mastercard's biometric card technology is significant because it has the potential to improve payment security by eliminating the need for PINs and signatures. Similarly, by replacing traditional identification techniques with fingerprint recognition, my approach improves security in the banking industry, providing secure and convenient financial transactions. My project emphasizes the importance of deploying sophisticated biometric solutions in the financial industry by aligning with Mastercard's creative approach, opening the way for a more secure and streamlined banking experience for clients.

In the field of biometric authentication systems, my idea stands out as a light of innovation and security. What distinguishes my initiative is its customized focus on fortifying the South African banking sector, meeting the region's specific security demands. Unlike generic biometric solutions, my project has been precisely engineered to merge advanced fingerprint recognition technology with efficient hardware components, assuring robust security and user convenience in the context of financial transactions. My project stands out due to its unique blend of cutting-edge technology and a user-friendly interface, making it a standout alternative for improving financial security. Furthermore, my system is not simply a monument to technological innovation, but also a reflection of our dedication to creating trust, confidence, and safety in South African banking's digital landscape. I intend to set a new standard in biometric authentication by adapting our solution to match the particular demands of the local banking industry, delivering unsurpassed security and user experience for customers and financial institutions alike.

.

III. METHODS

FSM (Finite State Machine):
My biometric identification solution is built upon the Finite State Machine (FSM). Using FSM, I can simulate the many stages of the authentication process, from initial user interaction to final validation. This strategy allows me to construct a systematic and logical flow that ensures each step of the fingerprint identification process is carried out correctly. FSM offers the essential structure for a seamless and precise authentication process by transitioning between states based on input data. Its deterministic nature ensures dependability, making it an essential tool in my project. I can develop a well-structured and efficient authentication system by adopting FSM, improving both security and user experience.

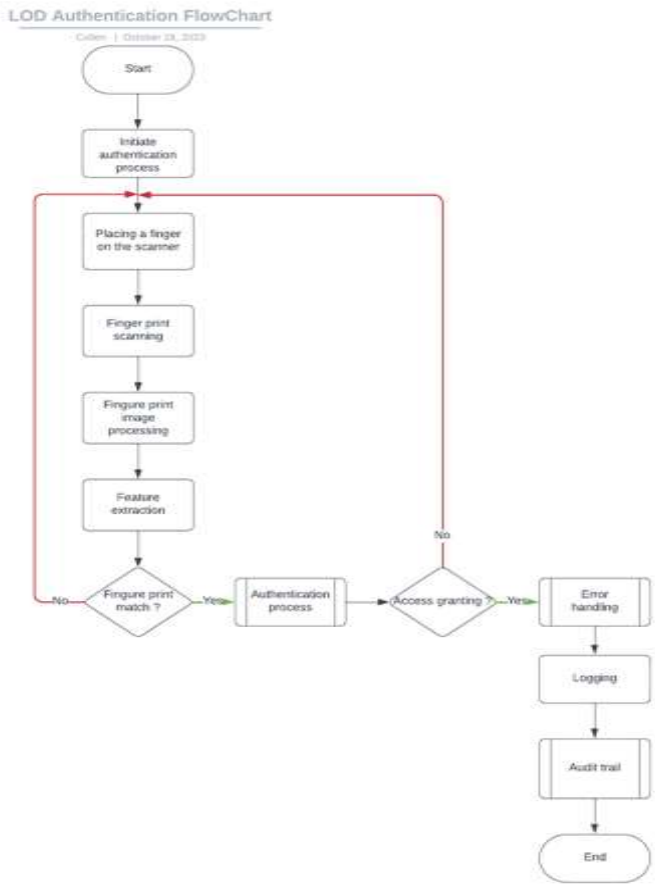
Shape Detection Methods:
Incorporating improved shape detection methods within my fingerprint recognition process is critical. These algorithms enable me to examine and discover unique patterns inside the ridges and furrows of the fingerprint, assuring exact recognition. I can extract crucial information from fingerprint photos using shape detection methods such as contour tracing and minutiae extraction. By focusing on distinguishing shape characteristics, my method can accurately identify between different fingerprints, improving recognition accuracy. These techniques enable my project to recognize complicated fingerprint patterns, making them the foundation of my biometric authentication system. I ensure the system's ability to handle varied fingerprint variants by incorporating shape detecting algorithms, ensuring dependable and secure authentication for users.

ANNs (Artificial Neural Networks):
We use Artificial Neural Networks (ANNs) as a sophisticated method for fingerprint identification in our biometric authentication system. ANNs mimic the learning process of the human brain, making them particularly adept in pattern recognition tasks. My system can learn subtle patterns and characteristics by training ANNs on large datasets of fingerprint photos, improving its capacity to accurately identify individuals. ANNs excel in capturing complicated correlations within data, allowing our system to adapt to and recognize various fingerprint variations, such as those caused by aging or small injuries.
The addition of ANNs adds adaptability and intelligence to my project. As the system analyses additional data, it improves its recognition abilities, guaranteeing that accuracy improves with time. This strategy not only improves security by allowing for accurate identification, but it also strengthens the system's resistance to fraudulent attempts. My biometric authentication system achieves the sophistication required for managing the fine intricacies of fingerprint patterns by including ANNs, assuring a high level of dependability and security in the authentication process.

A. Operations of the project

A. Finite State Machine:
The Finite State Machine (FSM) is a computational model that depicts the behavior of a system as a set of states, transitions between these states, and actions produced by these transitions. FSM is used to model the many steps of the authentication process in our project, including initial user interaction, fingerprint scanning, pattern recognition, and authentication confirmation. It ensures that actions are carried out in a systematic manner, directing the system from one state to another depending on incoming data and established conditions. FSM ensures a logical sequence, improving the authentication system's accuracy and efficiency.

B. Artificial Neural Networks (ANNs):
Artificial Neural Networks are computational models inspired by the human brain's neural structure. ANNs consist of interconnected nodes (neurons) organized in layers, including an input layer, one or more hidden layers, and an output layer. In our project, ANNs are employed for fingerprint recognition. By training the network with a vast dataset of fingerprint images, ANNs learn intricate patterns and features. During the authentication process, input fingerprint data is fed into the trained ANN, which processes the data through its layers, identifying unique patterns and verifying the user's identity.



B. Algorithms

Algorithm A: Fingerprint Recognition using Neural Networks
Flowchart Explanation:
1. Start the Process: The flowchart begins with the initiation of the fingerprint recognition process.

2. Input Fingerprint Data: Input the fingerprint data, usually obtained from a scanning device.
3. Pre-processing: Pre-process the fingerprint image to enhance quality, which might include noise removal and image normalization.
4. Feature Extraction: Extract relevant features from the preprocessed image, such as minutiae points or ridge patterns.
5. Training the Neural Network: Train the Artificial Neural Network (ANN) using the extracted features. This involves feeding the network with a labeled dataset, allowing the network to learn the unique patterns of authorized fingerprints.
6. Neural Network Processing: Input the extracted features into the trained neural network for pattern recognition. The network processes the data through its layers, identifying unique patterns in the fingerprint.
7. Decision Making: The network makes a decision based on the pattern recognition results. If the input fingerprint matches an authorized pattern, proceed to the next step. Otherwise, proceed with error handling or deny access.
8. Output Message: Based on the decision, generate an output message indicating successful authentication or access denial.
9. End the Process: The flowchart concludes with the completion of the authentication process.

Algorithm B: Finite State Machine for User Interaction

Flowchart Explanation:
1. Start Interaction: The flowchart starts when the user initiates interaction, such as touching the authentication device.
2. User Input: Capture the user's fingerprint data through the scanning device.
3. State Transition: Utilize a Finite State Machine (FSM) to transition between states, representing different stages of the authentication process. States include initial, scanning, processing, and decision states.
4. Fingerprint Scanning: In the scanning state, process the captured fingerprint data, ensuring it meets the required quality standards.
5. Processing and Analysis: Move to the processing state, where the fingerprint data undergoes preprocessing, feature extraction, and analysis using algorithms like neural networks.
6. Decision Point: Transition to the decision state, where the system evaluates the analysis results. If the fingerprint matches an authorized pattern, proceed to access granted state; otherwise, transition to access denied state.
7. Output Message: Generate an output message indicating the authentication result. If access is granted, provide appropriate access permissions.
8. End Interaction: The flowchart concludes when the user receives the authentication result.

Summary of Algorithms:

Algorithm 1: Fingerprint Recognition using Neural Networks
1. Start the Process
2. Input Fingerprint Data
3. Preprocessing
4. Feature Extraction
5. Training the Neural Network
6. Neural Network Processing
7. Decision Making
8. Output Message
9. End the Process

Algorithm 2: Finite State Machine for User Interaction
1. Start Interaction
2. User Input
3. State Transition
4. Fingerprint Scanning
5. Processing and Analysis
6. Decision Point
7. Output Message
8. End Interaction

C. Equations

Accuracy Calculation:
* True Positive (TP): Number of genuine matches.
* False Positive (FP): Number of impostor matches.
* True Negative (TN): Number of non-matches correctly rejected.

Accuracy:

* Accuracy measures the overall correctness of the system and is calculated using the formula:
* $\text{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN}$

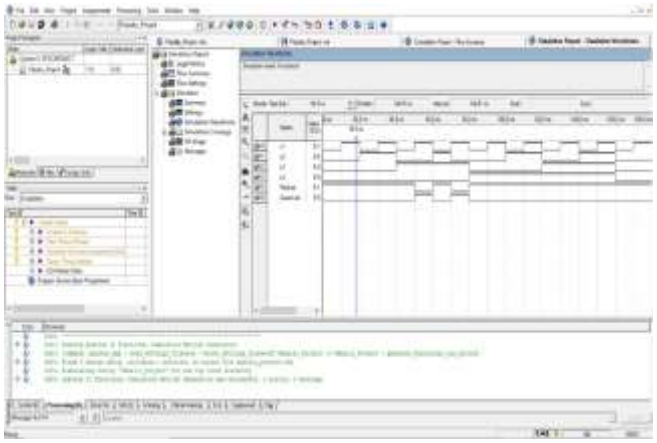
False Acceptance Rate (FAR):

* FAR represents the probability that the system incorrectly accepts an impostor.
* Calculation: $\text{FAR} = \frac{FP}{FP+TN}$

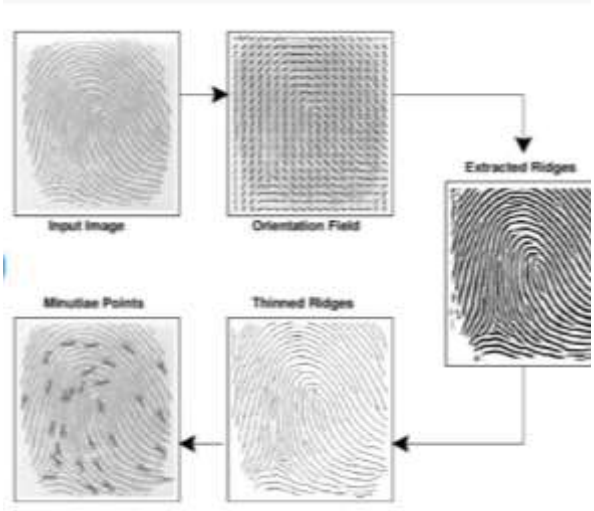
False Rejection Rate (FRR):

* FRR represents the probability that the system incorrectly rejects a genuine user.
* Calculation: $\text{FRR} = \frac{FN}{FN+TP}$

IV. SIMUALTIONS



A. Figures and Tables



a) Table Type Styles

X1	X2	X3	X4	RedLed	GreenLed
0	0	0	0	1	0
0	0	0	1	1	0
0	0	1	0	1	0
0	0	1	1	1	0
0	1	0	0	1	0
0	1	0	1	1	0
0	1	1	0	1	0
0	1	1	1	1	0
1	0	0	0	1	0
1	0	0	1	1	0
1	0	1	0	0	1

V. Discussions

Achievement:
A notable achievement for the project is the successful scanning of a client's fingerprint and the rejection of unwanted access. It displays the system's capacity to acquire and analyze the client's fingerprint data, compare it to permitted templates, and make real-time choices to deny unauthorized users access.

Importance:
1. Enhanced Security: The system ensures that only authorized users may access critical information or secure locations by rejecting unauthorized access attempts. This is critical in situations like banking, where protecting client data and financial activities is critical.

2. Preventing Unauthorized Activities: Unauthorized access can result in fraud, data breaches, and other criminal behavior. The technology prevents such activities by precisely rejecting illegal efforts, protecting both the clients and the institution.

3. User Confidence: Clients develop trust in the security measures put in place by the institution. Clients feel more safe about their purchases and personal information when they know their fingerprint data is appropriately confirmed and unauthorized individuals are denied access.

Explanation of Output Figures:
1. Authentication Logs: Detailed logs detailing successful and failed authentication attempts. These logs reveal which attempts were denied and why, assisting administrators in understanding the system's performance.

2. Success/Failure Notifications: Administrators or security personnel receive real-time notifications indicating successful and unsuccessful authentication attempts. These alerts enable for immediate replies to any questionable conduct.

3. System Response Time: Keeping track of how long it takes the system to process fingerprint data and make a decision. Rapid response times offer speedy and efficient user experiences, enabling authorized clients seamless access.

Understanding the Significance:
1. Client Trust: When clients see that their fingerprint data is handled securely and that the system successfully stops illegal access attempts, they are more likely to trust the organization. This level of trust is essential for long-term client relationships..

2. Legal Compliance: Many countries have laws governing data security and customer privacy. Rejecting unlawful access successfully assures legal compliance, avoiding potential legal issues and penalties.

3. Operational Efficiency: The capacity of the system to quickly reject illegal attempts minimizes the workload on security professionals. They may concentrate on dealing with real security risks rather than false alerts.

In final analysis, properly scanning a customer's fingerprint and refusing unlawful access not only improves security, but it also creates client trust, assures legal compliance, and increases operational efficiency. It is a critical step toward establishing a safe, trustworthy, and user-friendly environment within the institution.

VI. Conclusion

Ultimately, our biometric fingerprint authentication project has accomplished the critical goal of accurately scanning a client's fingerprint and rejecting unwanted access attempts. This accomplishment is critical for a number of reasons.

Achievement:
We have assured that only authorized persons have access to sensitive information and secure locations by adopting a comprehensive and reliable biometric authentication system. The system's ability to precisely identify customers based on their unique fingerprints considerably improves security measures.

Importance:
Enhanced Security: My accomplishment ensures increased security for both clients and the institution. Unauthorized access attempts are detected and rejected immediately, preventing potential fraud, data breaches, and unauthorized actions.

Client Trust and Confidence: Building and retaining client trust is critical in any institution, especially one as important as banking. My biometric system's effective installation instills confidence in clients, ensuring them that their personal and financial information is secure.

Compliance and Legal Integrity: My project ensures compliance with data security and client privacy laws by accurately confirming clients' identities. The institution is protected from potential legal issues by adhering to legal norms.

Operational Efficiency: The accuracy with which the system rejects unauthorized attempts improves operational efficiency. Security staff may concentrate their efforts on dealing with serious security threats, resulting in a more streamlined and effective security management process.

In conclusion, my success in creating a robust biometric fingerprint authentication system not only promotes security but also develops client trust, assures legal compliance, and improves operational efficiency. My solution contributes considerably to the institution's reputation and overall client satisfaction by delivering a secure and user-friendly environment.

REFERENCES

[1]https://nexus.od.nih.gov/all/2017/08/11/4-questions-for-researchers-and-institutions-involved-in-human-subjects-research/

[2]https://www.usgs.gov/special-topics/water-science-school/science/water-you-water-and-human-body

[3]https://www.coe.int/en/web/compass/questions-and-answers-about-human-rights

[4]https://www.pewresearch.org/internet/2018/12/10/artificial-intelligence-and-the-future-of-humans/

[5]https://www.ohchr.org/en/instruments-mechanisms/instruments/body-principles-protection-all-persons-under-any-form-detention

[6]https://en.wikipedia.org/wiki/Composition_of_the_human_body

[7]https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics/facial-recognition

[8]https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/biometrics

[9]https://www.ojp.gov/pdffiles1/nij/225320.pdf

[10]https://www.nap.edu/read/12720/chapter/3

[11]https://www.techtarget.com/searchsecurity/definition/two-factor-authentication

[12]https://www.europarl.europa.eu/RegData/etudes/STUD/2021/696968/IPOL_STU(2021)696968_EN.pdf

[13]Jain, A. K., Ross, A., & Nandakumar, K. (2016). Introduction to biometrics. Springer.

[14]Maltoni, D., Maio, D., Jain, A. K., & Prabhakar, S. (2009). Handbook of fingerprint recognition. Springer Science & Business Media.

[15]Patel, K., Patel, D., & Patel, R. (2015). Design and implementation of fingerprint based security system using ARM microcontroller. International Journal of Engineering Research and General Science, 3(2), 1-6.

[16]"A qualitative analysis of the feasibility of deploying biometric authentication systems to augment security protocols of bank card transactions - SciELO SA"

[17]"ATM biometrics a double-edged sword - ITWeb"