IJARST
International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

A SECURE AND ROBUST INDEXING ALGORITHM TO PROVIDE SECURITY WITH FINGERPRINTS

BHAGYALAKSHMI HASYAPU[1], K. PRANATI[2], SK. KARISHMA[3]

[1]Assistant Professor, Department of ECE, Mallareddy Engineering College For Women

[2,3]UG Scholar, Department of ECE, Mallareddy Engineering College For Women

ABSTRACT

Fingerprint security systems have become an integral part of modern biometric authentication, providing secure and reliable identification methods. However, one of the most critical challenges in such systems is the presence of distorted fingerprints, which can lead to significant errors in recognition, compromising both accuracy and reliability. This paper presents a novel two-phase framework designed to effectively address the issue of fingerprint distortion. The proposed system includes a classification phase and a distortion rectification phase, working together to ensure accurate recognition even in the presence of distortions. In the classification phase, fingerprints are analyzed to detect distortions using a feature vector developed from the registered orientation map. To improve the accuracy and efficiency of classification, a Feed Forward Neural Network (FFNN) is employed instead of the commonly used Support Vector Machine (SVM). The FFNN model enhances the system's ability to differentiate between distorted and undistorted fingerprints with higher precision. Once the distorted fingerprints are identified, they are passed to the distortion rectification phase, where distortion fields are estimated and corrected to restore the fingerprint's original structure. The effectiveness of the proposed system is evaluated through comparative experiments against existing methods. Key performance metrics such as False Acceptance Rate (FAR), True Acceptance Rate (TAR), and overall accuracy are used to measure the system's performance. Results indicate that the proposed approach outperforms traditional systems in all metrics, significantly reducing FAR while achieving higher TAR and overall accuracy. These improvements highlight the robustness and reliability of the proposed framework in addressing the challenges associated with distorted fingerprints. This research introduces a transformative solution to fingerprint security systems, addressing a long-standing limitation that has hindered their efficiency. By integrating advanced neural network techniques with distortion rectification methods, the system demonstrates enhanced performance in both identification accuracy and processing efficiency. Furthermore, the proposed framework is scalable and can be extended to diverse biometric security applications, ensuring broad applicability and usability in real-world scenarios. The proposed method not only mitigates the risks associated with fingerprint distortion but also sets a new benchmark for performance in fingerprint recognition systems. Its ability to adapt to varying levels of distortion makes it an ideal solution for high-security environments requiring robust and reliable biometric authentication. This contribution

provides a foundation for further exploration and development in the field of biometric security, paving the way for more advanced, distortion-resilient fingerprint recognition technologies.

INTRODUCTION

Fingerprint-based security systems are one of the most widely used biometric identification techniques due to their uniqueness, reliability, and convenience. A fingerprint is essentially an impression of the friction ridges of a finger, encompassing distinct structures like ridges and valleys. These epidermal ridges are formed by the interaction between the interpapillary pegs of the epidermis and the dermal papillae. Such intricate patterns are the foundation for fingerprint identification, but they are also sensitive to various factors that can distort their appearance. Distortion in fingerprints arises due to nonlinear transformations in ridge shapes caused by diverse factors, such as the angle and pressure of the finger on the sensor, skin condition (dry, moist, or oily), behavioral inconsistencies, and physical flexibility of the skin. These distortions can significantly impact the performance of fingerprint recognition systems, making it critical to address these challenges effectively. Low-quality fingerprints, whether due to geometric distortions or photometric degradations, pose a significant threat to the reliability of fingerprint-based systems. Fingerprint recognition systems are broadly categorized into positive and negative identification systems. Positive systems, such as those used in access control, aim to identify cooperative users who wish to be recognized. In contrast, negative systems, such as those used for identifying individuals in watchlists or preventing fraudulent registrations, must contend with uncooperative users who may deliberately degrade fingerprint quality to evade detection. For instance, law enforcement agencies often encounter criminals who damage or alter their fingerprints to avoid identification. The implications of low-quality fingerprints vary across these systems. In identification, poor-quality fingerprints can lead to the false rejection of genuine users, causing inconvenience and reducing system efficiency. In negative identification systems, the consequences are more severe, as malicious users can exploit the system's vulnerabilities by intentionally degrading fingerprint quality, potentially compromising security. Therefore, improving the robustness of fingerprint recognition systems against low-quality inputs is essential for maintaining their reliability. While photometric degradation caused by factors like lighting or sensor quality has been extensively studied, geometrical degradation due to skin distortion remains an underexplored challenge. Skin distortion, often resulting from bending or pressure variations, can significantly alter the spatial arrangement of ridges and valleys, leading to mismatches in automated fingerprint recognition systems. Addressing this issue is critical, as the security of a fingerprint system is only as strong as its ability to handle its weakest point—distorted fingerprints. This project aims to tackle the problem of fingerprint distortion through an efficient two-phase approach encompassing distortion detection and rectification. The proposed system identifies distorted fingerprints using advanced feature extraction techniques and rectifies them by estimating and compensating for distortion fields. By enhancing the quality of low-standard fingerprints, this method ensures that fingerprint recognition systems remain secure and effective even in the presence of challenging inputs. This research contributes to advancing fingerprint-based security systems by addressing a critical gap in their reliability and robustness.

LITERATURE SURVEY

A) G. Babatunde, A. O.Charles, A. B. Kayode, and O. Olatubosun, "Fingerprint Image Enhancement: Segmentation to Thinning", IJACSA, Vol.3, no.1, pp.15-24,2012.

Fingerprint recognition systems require high-quality images for accurate identification, but raw fingerprint images often suffer from poor contrast, noise, and incomplete ridge patterns. This paper presents a comprehensive approach to fingerprint image enhancement, focusing on segmentation, normalization, and thinning techniques. Segmentation isolates the fingerprint region from the background, ensuring that only relevant data is processed. Normalization then standardizes intensity variations across the image, reducing noise and mitigating inconsistencies caused by sensor conditions or skin properties. Thinning, the final step, refines ridge patterns to a single-pixel width, preserving essential details for reliable minutiae extraction. Together, these methods improve fingerprint image clarity, contributing to enhanced recognition accuracy. The quality of fingerprint images is critical for the performance of automated recognition systems, as low-quality images can lead to incorrect matches or failed identifications. Enhancing fingerprint images involves refining the ridge and valley structures to ensure that the system can accurately extract and compare unique features. This study addresses the challenges in preprocessing fingerprint images, presenting a structured methodology to overcome issues such as noise, ridge discontinuities, and background interference. By focusing on key enhancement techniques—segmentation, normalization, and thinning—this approach provides a robust solution for improving fingerprint image quality. The results of the study validate the effectiveness of these techniques, showing significant improvements in the reliability and accuracy of fingerprint recognition systems, even under challenging conditions.

B) J. Choudhary, Dr.S. Sharma, J.S. Verma, "A New Framework for improving low Quality Fingerprint Images", IJCTA, Vol.2, no.6, pp. 1859 - 1866, 2011.

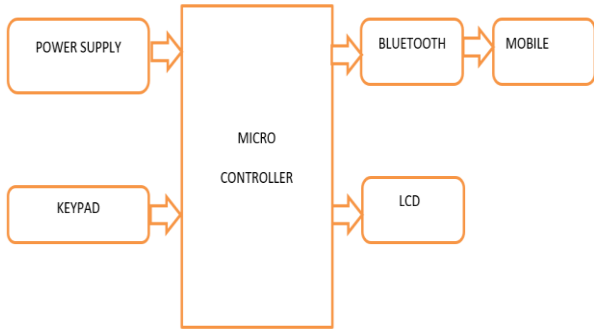
Low-quality fingerprint images pose significant challenges to automated fingerprint recognition systems, as they often contain noise, blurred ridge patterns, and inconsistent structures that hinder reliable feature extraction. This paper introduces a novel framework designed to enhance low-quality fingerprint images, ensuring better recognition accuracy. The proposed method combines advanced preprocessing techniques, including dynamic thresholding for noise reduction, adaptive contrast enhancement for improving ridge visibility, and contextual filtering to refine ridge continuity. Experimental evaluations demonstrate that the framework effectively transforms low-quality fingerprint images into usable data, resulting in substantial improvements in recognition performance across various datasets. Fingerprint recognition is a widely used biometric technique, but its effectiveness is heavily dependent on the quality of the input fingerprint images. Low-quality images, often caused by factors such as poor sensor conditions, dry or moist skin, or improper placement of the finger, result in degraded ridge patterns that complicate the identification process. Addressing these challenges requires robust enhancement methods capable of mitigating noise and inconsistencies while preserving critical fingerprint features. This study proposes an innovative framework for improving low-quality fingerprint images through a combination of preprocessing techniques that optimize ridge clarity and continuity. The results demonstrate that the proposed framework not only enhances image quality but also significantly improves the reliability and accuracy of fingerprint recognition systems, making it a valuable contribution to the field of biometric authentication.

C)Soweon Yoon, Jianjiang Feng, and Anil K. Jain, "On Latent Fingerprint Enhancement", Michigan State University, MI 48824, USA,2010.

Latent fingerprints, often encountered in forensic investigations, are among the most challenging biometric data to process due to their poor quality and incomplete ridge structures. This paper focuses on the enhancement of latent fingerprints to improve their utility in identification systems. The proposed methodology includes advanced image preprocessing techniques, such as noise reduction, ridge enhancement, and context-based filtering, designed to address the specific challenges posed by latent prints. Experimental results demonstrate that the enhanced latent fingerprints yield significant improvements in feature extraction and matching accuracy. This research provides valuable insights into overcoming the limitations of latent fingerprint quality, enhancing their usability in forensic and biometric applications. Latent fingerprints are impressions left unintentionally on surfaces, often found at crime scenes, and serve as critical evidence in forensic investigations. Unlike rolled or plain fingerprints, latent prints are typically of poor quality, exhibiting incomplete ridge structures, smudges, and noise. These characteristics make latent fingerprints challenging for automated recognition systems, necessitating specialized enhancement techniques to extract usable features. The enhancement of latent fingerprints involves addressing their unique challenges, such as low contrast, ridge discontinuities, and background interference while preserving the critical ridge and valley patterns. This study aims to develop effective methods for latent fingerprint enhancement, leveraging advanced image processing algorithms tailored for forensic use. The proposed techniques are designed to minimize noise, enhance ridge clarity, and improve the overall quality of latent prints for feature extraction and matching. By addressing the inherent limitations of latent fingerprint quality, this research contributes to advancing the field of forensic biometrics, ensuring that latent fingerprints can be effectively used in identification and investigative processes Distorted fingerprints present significant challenges in biometric recognition systems, as they can lead to incorrect matches and undermine system reliability. The base paper titled *Detection and Rectification of Distorted Fingerprints using Geometric Features and FFNN* focuses on addressing this problem by introducing a systematic framework for detecting and correcting fingerprint distortions. This research is vital for ensuring the robustness and accuracy of fingerprint-based identification, especially in high-security applications. The proposed framework comprises two main stages: distortion detection and rectification. In the first stage, the system analyzes geometric features of the fingerprint, such as the orientation map, period map, and regional characteristics, to detect distortions. The orientation map captures the directional flow of ridges, while the period map represents the spacing between ridges. Regional features, derived from specific areas of the fingerprint, provide additional data for analyzing distortions. These features are extracted and processed to create a robust feature vector that characterizes the level of distortion in the input fingerprint image. For classification, the study leverages a Feed Forward Neural Network (FFNN), which is a significant improvement over traditional Support Vector Machine (SVM) classifiers. FFNNs excel in handling complex and nonlinear datasets, making them particularly effective for analyzing distorted fingerprint patterns. The FFNN classifier assigns input fingerprints to one of two categories: distorted or non-distorted. This step ensures that only problematic fingerprints are passed to the next stage for rectification, optimizing computational efficiency. In the second stage, the detected distorted fingerprints undergo rectification through the estimation of distortion fields. This process involves analyzing the geometric inconsistencies identified in the first stage and applying corrections to restore the original ridge patterns. The rectification algorithm focuses on aligning the distorted ridges and valleys to their natural positions without losing critical fingerprint details. By addressing distortions at the structural level, the framework ensures that the rectified fingerprints maintain their integrity and usability for feature extraction and matching. The effectiveness of this framework is demonstrated through extensive simulations and evaluations using performance metrics such as False Acceptance Rate (FAR), True Acceptance Rate (TAR), and overall accuracy. The results highlight the superiority of the proposed method compared to existing approaches, with significant reductions in FAR and improvements in TAR and accuracy. These advancements underscore the framework's potential to enhance the reliability of fingerprint recognition systems, even in the presence of severe distortions.One of the key strengths of this study is its focus on practical applications. Distorted fingerprints are not only a technical challenge but also a security vulnerability that can be exploited by malicious actors, such as criminals attempting to evade detection by deliberately distorting their fingerprints. By developing a robust system for detecting and rectifying these distortions, the research addresses a critical gap in the field of biometric security.The paper also emphasizes the importance of future work in this domain. While the proposed framework effectively handles distortion detection and rectification, integrating it with a comprehensive fingerprint recognition system would create an end-to-end solution capable of handling diverse challenges in biometric identification. This could include further optimization of the FFNN classifier, advancements in rectification algorithms, and testing the framework across a broader range of real-world scenarios.In summary, the study *Detection and Rectification of Distorted Fingerprints using Geometric Features and FFNN* represents a significant contribution to the field of biometric security. By combining geometric feature analysis with advanced neural network classification, it provides an effective solution to one of the most persistent challenges in fingerprint recognition. This research not only improves the accuracy and robustness of fingerprint systems but also enhances their applicability in high-stakes security environments.

IMPLEMENTATION

BLOCK DIAGRAM



POWER SUPPLY

A **regulated power supply** transforms unregulated AC (Alternating Current) into a stable DC (Direct Current). It guarantees consistent output despite variations in input. A regulated DC power supply is also known as a linear power supply, it is an embedded circuit and consists of various blocks

- **Regulated Power Supply Definition**: A regulated power supply ensures a consistent DC output by converting fluctuating AC input.
- **Component Overview**: The primary components of a regulated power supply include a transformer, rectifier, filter, and regulator, each crucial for maintaining steady DC output.
- **Rectification Explained**: The process involves diodes converting AC to DC, typically using full wave rectification to enhance efficiency.
- **Filter Function**: Filters, such as capacitor and LC types, smooth the DC output to reduce ripple and provide a stable voltage.
- **Regulation Mechanism**: Regulators adjust and stabilize output voltage to protect against input changes or load variations, essential for reliable power supply

SENSORS

Sensors are used for sensing things and devices etc. A device that provides a usable output in response to a specified measurement. The sensor attains a physical parameter and converts it into a signal suitable for processing (e.g. electrical, mechanical, optical) the characteristics of any device or material to detect the presence of a particular physical quantity. The output of the sensor is a signal which is converted to a human-readable form like changes in characteristics, changes in resistance, capacitance, impedance, etc.

FINGERPRINT MODULE

Description

KY-M6 Fingerprint module adopts optic fingerprint sensor, which consists of high-performance DSP and Flash.

***Introduction**

KY-M6 Fingerprint Sensor Module is able to conduct fingerprint image processing, template generation, template matching, fingerprint searching, template storage, etc. Compared with similar products from other suppliers, KY-M6 proudly boasts of following features:

1. Proprietary Intellectual Property

Optic fingerprint enrollment device, KY-M6 hardware as well as fingerprint algorithm are all developed by KeyPower Security.

2. Wide Application Range of Fingerprints with Different Quality

Self-adaptive parameter adjustment mechanism is used in the course of fingerprint enrollment. This ensures good image quality for even dry or wet fingers, thus it has wider application range.

3. Immense Improved Algorithm

KY-M6 Fingerprint algorithm is specially written according to optic imaging theory. The algorithm is good for low-quality fingers due to its excellent correction and tolerance features.

4. Flexible Application

User can easily set KY-M6 Module to different working modes depending on complexity of application systems. User can conduct secondary development with high efficiency and reliability.

5. Easy to Use and Expand

It is not necessary for user to have professional knowledge in the field of fingerprint verification. User can develop powerful fingerprint verification application systems with the command set provided by KY-M6.

6. Low Power Consumption

Sleep/awake control interface makes KY-M6 suitable for occasions that require low power consumption.

7. Different Security Levels

User can set different security level according to different application environment.

8. Application

KY-M6 can be used on all fingerprint verification systems, such as Safety cabinet, door lock, Complicated door-guard system, Fingerprint IC card Identification Terminal, Fingerprint identification and verification system associated with PC.

NODEMCU:

NodeMCU is an open source LUA based firmware developed for ESP8266 wifi chip. By exploring functionality with ESP8266 chip, NodeMCU firmware comes with ESP8266 Development board/kit i.e. NodeMCU Development board. Since NodeMCU is open source platform, their hardware design is open for edit/modify/build. NodeMCU Dev Kit/board consist of ESP8266 wifi enabled chip. The ESP8266 is a low-cost Wi-Fi chip developed by Espressif Systems with TCP/IP protocol. For more information about ESP8266, you can refer ESP8266 WiFi Module. There is Version2 (V2) available for NodeMCU Dev Kit i.e. NodeMCU Development Board v1.0 (Version2), which usually comes in black colored PCB.

NodeMCU Development Kit/Board consist of ESP8266 wifi chip. ESP8266 chip has GPIO pins, serial communication protocol, etc. features on it.

ESP8266 is a low-cost Wi-Fi chip developed by Espressif Systems with TCP/IP protocol. For more information about ESP8266, you can refer ESP8266 WiFi Module.

The features of ESP8266 are extracted on NodeMCU Development board. NodeMCU (LUA based firmware) with Development board/kit that consist of ESP8266 (wifi enabled chip) chip combines NodeMCU Development board which make it stand-alone device in IoT applications.

Let’s see 1st version of NodeMCU Dev Kit and its pinout as shown in below images.

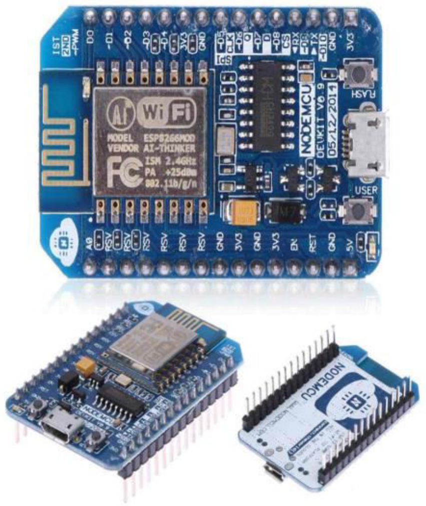


Fig: Node Mcu

CONCLUSION

In this research, we proposed an innovative framework for automatic detection and rectification of fingerprint image distortions using orientation maps, period maps, and regional feature extraction. By employing a Feed Forward Neural Network (FFNN) for classification instead of traditional SVM classifiers, the system effectively addressed the high false non-match rates associated with severely distorted fingerprints. The results demonstrate that the proposed approach significantly reduces the affirmation gap in automatic fingerprint recognition systems, enhancing their reliability and robustness. This advancement is particularly critical in applications requiring heightened security, where distorted fingerprints could otherwise be exploited by malicious actors. The simulation results validate the effectiveness of the proposed framework, showing marked improvements over existing methods in distortion detection and rectification accuracy. This study not only addresses a critical weakness in fingerprint recognition systems but also lays the groundwork for future enhancements. For subsequent research, we recommend extending this framework to develop a comprehensive end-to-end fingerprint recognition system that integrates distortion rectification seamlessly with feature extraction and matching, further improving its applicability in real-world biometric security scenarios.

REFERENCES

[1] I. G. Babatunde, A. O.Charles, A. B. Kayode, and O. Olatubosun, “Fingerprint Image Enhancement: Segmentation to Thinning”,IJACSA, Vol.3,no.1, pp.15-24,2012.

[2] J. Choudhary, Dr.S. Sharma, J.S. Verma, “A New Framework for improving low Quality Fingerprint Images”, IJCTA, Vol.2, no.6, pp. 1859 -1866, 2011.

[3] Soweon Yoon, Jianjiang Feng and Anil K. Jain, "On Latent Fingerprint Enhancement",Michigan State University, MI 48824, USA,2010.

[4] Xue Jun-tao, Liu Jie & Liu Zheng-guang, "An enhancement algorithm for low quality fingerprint image based on edge filter and Gabor filter", Proc. of SPIE, Vol. 7383, 2009.

[5] Dinesh Kumar Misra, Dr S.P. Tripathi, "Fingerprint Image Enhancement Based on Energy Minimisation Principle", IJCSC, Vol.3, no.1, pp.165-170, 2012.

[6] C.Nandini, C.N.Ravikumar, "Improved Fingerprint Image representation for recognition," IJCSIT, MIT Publication, Vol. 01, no.2, pp.59-64, 2011.

[7] P.Sutthiwichaiporn,V. Areekul, and S. Jirachaweng, "Iterative Fingerprint Enhancement with Matched Filtering and Quality Diffusion in Spatial-Frequency Domain", ICPR, DOI 10.1109/ICPR.2010.313,pp.1257-1260,20107.

[8] Andelija M. Raicevic and Brankica M. Popovic, "An Effective and Robust Fingerprint Enhancement by Adaptive Filtering in Frequency Domain",FACTA Universities conference, Vol.22, No.1, pp.91-104,2009.

[9] K. Srinivasan, C. Chandrasekar,"An Efficient Fuzzy Based Filtering Technique for Fingerprint Image Enhancement", AJSR,ISSN 1450-223X, no.43, pp. 125-140, 2012.

[10] D.Bennet and Dr. S. Arumuga Perumal, "Fingerprint: DWT, SVD Based Enhancement and Significant Contrast for Ridges and Valleys Using Fuzzy Measures", JCSE, Vol. 6, no.1, pp.36-42, 2011

[11] Tanaya Mandal and Q. M. Jonathan Wu, "A Small Scale Fingerprint Matching Scheme Using Digital Curvelet Transform",IEEE Conf. on SMC,pp.1534-1538,2008.

[12] Sharat S. Chikkerur, Alexander N. Cartwright and Venu Govindaraju, "Fingerprint Image Enhancement using STFT Analsis",Pattern Recognition,Vol.40,pp. 198-211,2007.

[13] Mohd Shahrimie Mohd Asaari ; Shahrel Azmin Suandi ; Bakhtiar Affendi Rosdi, "Geometric feature extraction by FTAs for finger based biometrics system", IET Biometrics (Volume: 6, Issue: 3, 5 2017), 2017.

[14] Celia Cintas ; Mirsha Quinto-Sánchez ; Victor Acuña ; Carolina Paschetta ; Soledad de Azevedo ; Caio Cesar Silva de Cerqueira ; Virginia Ramallo ; Carla Gallo ; Giovanni Poletti ; Maria Catira Bortolini ; Samuel Canizales-Quinteros ; Francisco Rothhammer ; Gabriel Bedoya ; Andres Ruiz-Linares ; Rolando Gonzalez-José ; Claudio Delrieux, "Automatic ear detection and feature extraction using Geometric Morphometrics and convolutional neural networks", IET Biometrics (Volume: 6, Issue: 3, 5 2017), 2017.

[15] Bo Wu ; Sridhar Sri Krishnan ; Nan Zhang ; Li Su, "Compact and robust video fingerprinting using sparse