Fingerprint Identification in Self-Lending System Using Support Vector Machine

Rangga Putra Aidani[1], Dr. Iman Fahruzi, S.T., M.T.[1*]

[1]Department of Electrical Engineering, Electronics Engineering Technology Study Program, Politeknik Negeri Batam, Batam, Indonesia

[*]Email:ranggapa78@gmail.com

Abstrak- The self-service borrowing system is an innovative service that allows users to borrow laboratory equipment without direct involvement from staff. The traditional system with manual recording is considered inefficient because it is prone to recording errors, the risk of losing forms, and long queues. This study aims to develop a self-service borrowing system that integrates fingerprint biometric technology for security authentication and QR codes for automated item recording. The user identification process is carried out through feature extraction using Histogram of Oriented Gradients (HOG), which is then classified with a Support Vector Machine (SVM) algorithm based on Radial Basis Function (RBF) kernel on a Raspberry Pi device. The test results show that the SVM model successfully achieved a training accuracy of 94.7%. In direct system testing (1:N identification), the system achieved an accuracy of 94.06% with a False Rejection Rate (FRR) of 6% and a False Acceptance Rate (FAR) of 7%. All QR Code scans of items were successfully performed and directed to the database system in realtime. This system has proven effective in enhancing the security and efficiency of laboratory equipment management through service automation.

Keyword: Fingerprint Identification, Support Vector Machine (SVM), Self-Service Borrowing System, QR Code

I. INTRODUCTION

Laboratory equipment represents a primary facility with a strategic role in supporting practicum activities, research, and competency development of students in higher education environments. The availability of adequate laboratory equipment, managed in an orderly manner and properly recorded, contributes significantly to the smooth running of learning processes and experiments conducted by both students and lecturers. Proper equipment management also plays an important role in maintaining optimal equipment conditions, minimizing damage, and ensuring accountability in the use of laboratory equipment. However, in practice, the majority of educational institutions still employ conventional borrowing systems based on paper forms or manual recording by laboratory staff. Such management methods are highly susceptible to various problems, including loss of borrowing data, recording errors, delays in data updates, and difficulties in tracking equipment borrowing history. Furthermore, the direct involvement of staff in verifying user identity and recording items often creates long queues, particularly during peak hours when many students borrow equipment simultaneously, thereby reducing the efficiency of laboratory services.

As a solution to these challenges, several educational institutions have begun implementing technology-based borrowing systems, such as Radio Frequency Identification (RFID) and Quick Response Code (QR Code). RFID systems enable users to complete the borrowing process simply by bringing an RFID card close to a scanner, allowing identification and data recording to be performed automatically and more rapidly. Meanwhile, QR Codes are utilized to simplify the identification and recording of borrowed items, as each piece of equipment can be assigned a unique code that is easily scanned. For instance, research conducted by Choerudin et al. demonstrated that the implementation of an RFID-based borrowing system was capable of accelerating the borrowing process and enabling automatic data recording compared to manual systems. Nevertheless, that study also revealed a security weakness, as RFID systems remain dependent on the physical possession of cards that could potentially be lent out, lost, or misused by unauthorized parties [15].

Another study conducted by Jaya et al. implemented a QR Code-based borrowing system to optimize laboratory inventory management. The results indicated that the use of QR Codes was able to improve the efficiency of the equipment borrowing and return process, as well as facilitate digital recording of inventory data. However, the developed system still employed basic authentication mechanisms, such as manually entered user identities, without any biometric-based identity verification. This condition caused the system to be not yet fully capable of guaranteeing the security of equipment usage, as there remained opportunities for misuse by unauthorized users or the use of another person's identity by other parties [1].

Based on the weaknesses identified in both systems, this study proposes the design of a laboratory borrowing system that integrates two main technological components, namely biometric verification using fingerprints as a user authentication mechanism, and QR Code scanning for the recording and validation of borrowed items. The use of fingerprint biometrics is considered more secure and reliable because fingerprints possess unique characteristics for each individual, are permanent in nature, are not easily falsified, and cannot be transferred to another person. Research conducted by Putra et al. proved that fingerprints possess universal, unique, and permanent characteristics, and can be recognized even using simple devices such as mobile phone cameras. By applying a minutiae-based feature extraction method and minutiae matching technique, the system developed in that study was able to achieve an identification accuracy rate of up to 95.3% [2].

In the proposed system, the user's fingerprint image is processed through several stages, beginning with an image preprocessing stage to enhance image quality, followed by a feature extraction stage using Gabor filters and Histogram of Oriented Gradients (HOG) to obtain distinctive texture patterns that represent the unique characteristics of each user's fingerprint. The features generated from this process are subsequently classified using a Support Vector Machine (SVM) algorithm to automatically and accurately identify the user's identity. In the classification stage, SVM is implemented using a Radial Basis Function (RBF) kernel, which functions to handle nonlinear data patterns in fingerprint features, thereby enabling more optimal separation between classes. Once the biometric verification process is successfully completed, users can independently borrow equipment by scanning the QR Code attached to the laboratory equipment as a form of item validation. Through this approach, the developed system is not only capable of reducing dependence on laboratory staff, but also accelerates the borrowing transaction process, minimizes queues, improves the efficiency of digital inventory management, and strengthens the security aspect, as only biometrically verified users are permitted to access and borrow laboratory equipment.

II. Method

A. System Design Diagram

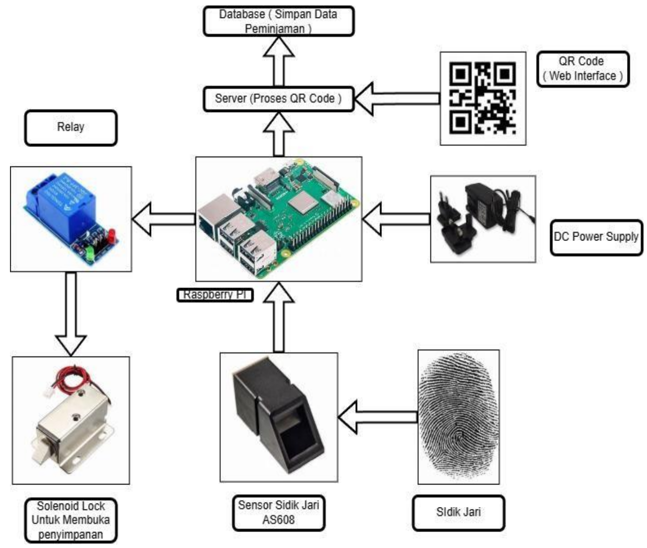


Figure 1. System Design Diagram

Figure 1 illustrates the overall architecture of the proposed system. This system employs a centralized architecture with the Raspberry Pi as the main microcontroller that coordinates all components. The AS608 fingerprint sensor functions as the primary user authentication method with direct communication to the Raspberry Pi via a serial protocol, while the QR Code scanner provides an alternative access method through a web interface using an HTTP request protocol to the server. The Raspberry Pi performs user data verification and controls the relay module for the storage unlocking mechanism. The server acts as the central data processing unit that handles QR Code requests, while the database stores all user information, booking status, and system activity logs that can be accessed in real-time for monitoring purposes.

B. Dataset and Data Augmentation

Figure 3. Dataset and Data Augmentation

Figure 8 shows sample fingerprint images captured from one of the registered users, labeled f1 through f5, representing the original scan along with its four augmented variations used for model training. The dataset used in this study consists of fingerprint images collected directly from 10 users using the AS608 fingerprint sensor, with 5 images per user, resulting in a total of 50 training images. Each image was captured at a resolution of 256 × 288 pixels in grayscale format and stored in .bmp format.

To enhance data variability and improve model generalization, each fingerprint image underwent a data augmentation process by simulating common real-world scanning conditions. Each scanned image was replicated into four additional variations, including weak and strong pressure simulations represented through intensity adjustments, as well as rotations of +10° and −10° to mimic differences in finger orientation during scanning. Consequently, each single fingerprint scan produced a total of five images, consisting of one original image and four augmented images. All augmented images were stored in a structured dataset folder organized by each respective user.

C. System Workflow Diagram

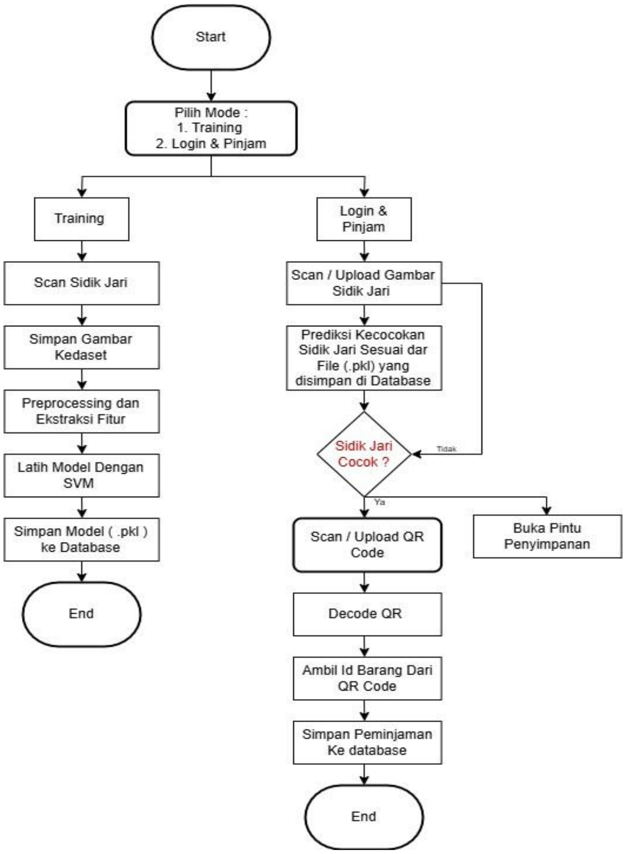


Figure 2. System Workflow Diagram

Figure 2 illustrates the overall workflow of the proposed system, which is divided into two main operational modes:Training Mode and Login & Borrow Mode.In the Training Mode, the process begins with scanning the user's fingerprint, which is then saved as an image into the dataset folder. The stored fingerprint images subsequently undergo preprocessing and feature extraction to enhance image quality and obtain distinctive fingerprint characteristics. These extracted features are then used to train the SVM classification model, and the resulting trained model is saved as a .pkl file into the database for later use during authentication.

In the Login & Borrow Mode, the user scans or uploads a fingerprint image, which is then matched against the trained model stored in the database. If the fingerprint is not recognized, the system denies access and the storage door remains locked. Conversely, if the fingerprint is successfully verified, the user proceeds to scan or upload a QR Code associated with the desired equipment. The system then decodes the QR Code to retrieve the item ID, and the borrowing transaction is recorded and saved into the database, while the storage door is unlocked to allow the user to retrieve the equipment.This dual-mode architecture ensures that the system maintains both flexibility in model management and security in equipment access control.

D. Fingerprint Model Training Workflow

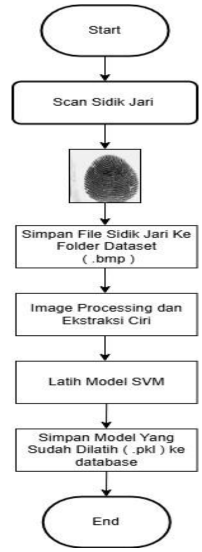


Figure 4. Fingerprint Model Training Workflow

Figure 4 illustrates the workflow of the Training Mode in the proposed system. The process begins with scanning the user's fingerprint using the AS608 sensor, and the captured image is saved into the dataset folder in .bmp format. The stored image then undergoes preprocessing and feature extraction using Gabor filters and HOG to obtain distinctive fingerprint characteristics. These extracted features are subsequently used to train the SVM classification model, and the resulting trained model is saved as a .pkl file into the database. This trained model will later be used as a reference for real-time fingerprint verification during the borrowing process, ensuring that only registered and authorized users are granted access to the laboratory equipment.

E. Mechanical Design

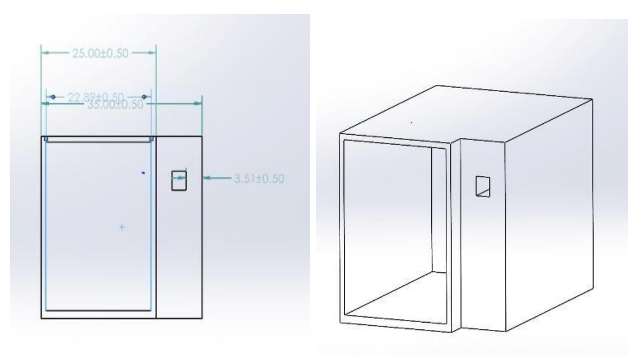


Figure 5. Mechanical Design

Figure 5 The mechanical design of this device features a main structure made of 3 mm thick acrylic, with a total width of 35 cm; the front face is divided into 25 cm and 10 cm sections to accommodate the solenoid lock. This construction includes a section on the side that serves as the location for the fingerprint sensor, where all dimensions have been precisely calculated to ensure structural rigidity and ease of integration of the electronic components within it.

F. Registered and Unregistered User Identification Testing

The fingerprint identification system was evaluated through two main scenarios to assess the system's ability to distinguish between authorized and unauthorized users. In the first scenario, registered users who had completed the registration process and had their fingerprint data stored in the system dataset performed 10 identification attempts each to measure system consistency and reliability. In the second scenario, unregistered users whose fingerprints had never been registered into the system also performed 10 identification attempts to evaluate the system's capability in rejecting unauthorized access.

Kelas Sebenarnya	**Kelas Prediksi**	
	Positive	***Negative***
True	**TP**	**FN**
False	**FP**	**TN**

Table 1. Confusion Matrix Structure

The system produces four classification result categories as the basis for evaluation metric calculations:

a) True Positive (TP): The system correctly accepts a registered user and grants access.

b) False Negative (FN): The system incorrectly rejects a registered user who should have been accepted, preventing a legitimate user from accessing the system despite having authorization.

c) True Negative (TN): The system correctly rejects an unregistered user, successfully preventing unauthorized access.

d) False Positive (FP): The system incorrectly accepts an unregistered user, representing a critical security vulnerability as it grants access to an unauthorized party.

III. RESULTS AND DISCUSSION

A. Training Results

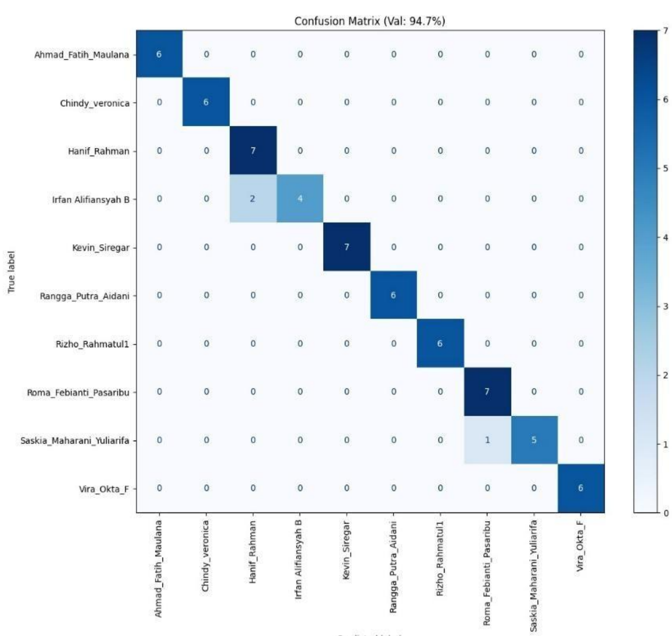
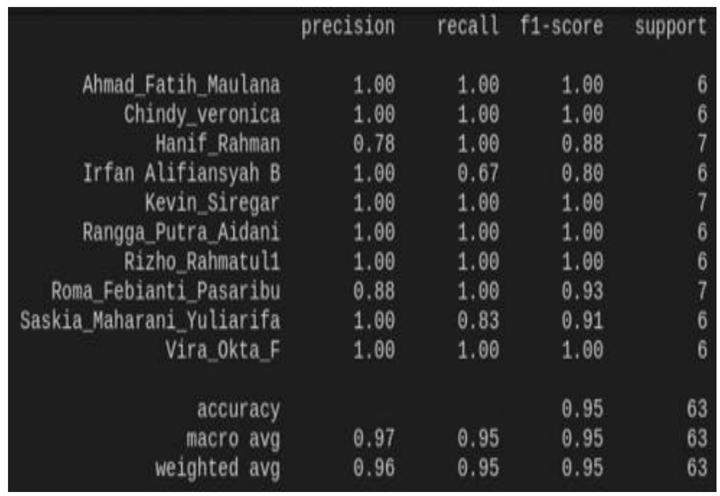


Figure 6. Confusion Matrix Model Results

Based on the test results shown in Figure 12, the developed Support Vector Machine (SVM) model demonstrates excellent performance with an accuracy rate of 94.7%. This is clearly reflected by the dominant values along the main diagonal of the confusion matrix, indicating that the system successfully recognizes the majority of fingerprint owners correctly. The Histogram of Oriented Gradients (HOG) feature extraction method proved highly effective in capturing ridge patterns and orientations specific to each individual, enabling accurate user identification.

Nearly all subjects, including Hanif Rahman, Kevin Siregar, and Vira Okta F, were identified perfectly without any misclassification. However, minor errors were still observed, where 2 samples of Irfan Alifiansyah B were misclassified as Hanif Rahman, and 1 sample of Saskia Maharani was incorrectly identified as Roma Febianti. These errors are most likely attributed to similarities in natural ridge pattern characteristics between individuals or imprecise finger positioning during scanning. These results extend the findings of Gian Nathan Christyo Nugroho (2024) by demonstrating that SVM is also effectively applicable to individual identification scenarios with a higher level of accuracy.



	precision	recall	f1-score	support
Ahmad_Fatih_Maulana	1.00	1.00	1.00	6
Chindy_veronica	1.00	1.00	1.00	6
Hanif_Rahman	0.78	1.00	0.88	7
Irfan Alifiansyah B	1.00	0.67	0.80	6
Kevin_Siregar	1.00	1.00	1.00	7
Rangga_Putra_Aidani	1.00	1.00	1.00	6
Rizho_Rahmatul1	1.00	1.00	1.00	6
Roma_Febianti_Pasaribu	0.88	1.00	0.93	7
Saskia_Maharani_Yuliarifa	1.00	0.83	0.91	6
Vira_Okta_F	1.00	1.00	1.00	6
accuracy			0.95	63
macro avg	0.97	0.95	0.95	63
weighted avg	0.96	0.95	0.95	63

|Figure 7. Visualization Terminal of Model Results

As shown in Figure 13, the SVM model with HOG feature extraction achieved an accuracy of 94.7% (rounded to 95%) across 63 test samples. This high performance is confirmed by the dominant values along the main diagonal of the confusion matrix, where most users such as Ahmad Fatih Maulana, Kevin Siregar, and Vira Okta F were identified perfectly with an F1-score of 1.00.

Minor misclassifications were observed in two cases: Irfan Alifiansyah B achieved a recall of 0.67 due to 2 samples being misclassified as Hanif Rahman, and Saskia Maharani achieved a recall of 0.83 as 1 sample was incorrectly identified as Roma Febianti. Overall, the consistently high precision and recall values across the majority of classes indicate that the model possesses good reliability in distinguishing unique fingerprint patterns between individuals.

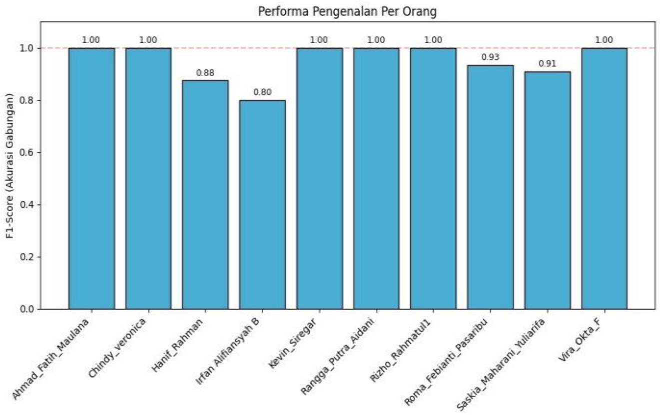


Figure 8. F1 Score Chart Model Results

As shown in Figure 8, the F1-Score graph demonstrates that the developed model exhibits excellent effectiveness, with the majority of users achieving a perfect F1-score of 1.00, including subjects such as Ahmad Fatih Maulana, Chindy Veronica, and Vira Okta F, indicating that HOG features successfully distinguished their fingerprint characteristics without any misclassification.

However, minor variations were observed in certain individuals. Irfan Alifiansyah B obtained an F1-score of 0.80 due to a low recall value, while Saskia Maharani Yuliarifa scored 0.91. Additionally, Hanif Rahman (0.88) and Roma Febianti (0.93) experienced reduced precision values as samples from other users were incorrectly detected under their identities. Overall, the weighted average F1-score of 0.95 confirms that the model is highly reliable and performs strongly in distinguishing unique fingerprint patterns across all registered users. Visualization of Fingerprint Identification System Testing.

B. Visualization of Fingerprint Identification System Testing

Figure 9. Results of Registered User Identification Testing

Figure 9 displays various test results when the system successfully recognizes fingerprints registered in the database. Each identification result is presented in a dialog box containing the identified user's name, a confidence score representing the system's certainty percentage in recognizing the fingerprint, and a confirmation message. The displayed confidence levels vary from 61.3% to 91.6%, reflecting the SVM algorithm's degree of certainty in classifying the scanned fingerprint against previously learned training data. The higher the confidence value, the more certain the system is that the fingerprint belongs to a specific registered user class, resulting in improved identification accuracy.

Figure 10. Results of Non Registered User Identification Testing

Figure 10 displays the test results when the system scans an unregistered fingerprint. On the left side of the figure, the system log shows the matching process against several registered users, returning confidence values of 23.19%, 37.61%, 29.46%, 39.33%, and 26.14%. All matching results display the status "[DECISION] REJECT (Low Confidence < 50.0%)", indicating that the system rejected the identification as all confidence values fell below the minimum threshold of 50%. As a result, the system displays a "Sidik Jari Tidak Dikenal!!" notification, informing the user that the scanned fingerprint could not be recognized. These results demonstrate that the implemented SVM algorithm is capable of effectively distinguishing between registered and unregistered fingerprints by applying a confidence threshold as the access rejection decision parameter.

C. Fingerprint Identification System Test Results

The registered user identification test was conducted to evaluate the system's ability to recognize users who have completed the registration process and have their fingerprint data stored in the dataset. The test involved 10 registered users, each performing 10 fingerprint identification attempts, resulting in a total of 100 trials. Each attempt was recorded as either a successful identification (True Positive/TP) or a failed recognition (False Negative/FN). The test results are presented in Table 2 below:

NO	Pengguna Terdaftar	Jumlah Pengujian	TP	FN	FRR (Total)
1	Rangga Putra Aidani	10	10	0	
2	Irfan Alifiansyah B		8	2	
3	Rizho Rahmatul		9	1	
4	Ahmad Fatih Maulana		10	0	
5	Kevin Siregar		9	1	
6	Saskia Maharani Y		9	1	
7	Roma Febianti P		10	0	
8	Chindy Veronica		10	0	
9	Hanif Rahman		10	0	
10	Vira Okta F		9	1	
	Total	100	94	6	5%

Table 2. Registered User Testing

Pengguna Tidak Terdaftar	Jumlah Pengujian	Threshold	Rata -Rata Confidence (%)	TN	FP	FAR Total %
Ikhsan Sabri	10	50	35,11%	8	2	
Ignasius Radja N			32,30%	10	0	
Raka Shabran			30,49%	10	0	
Agri Yuda			34,34%	8	2	
Ridho Al			31,99%	10	0	
Asnimar			31,25%	10	0	
Ainul Yakin			33,50%	9	1	
Muhammad Ghazi Allawie			36,41%	9	1	
Yogi Yudika S			31,84%	10	0	
Valent S			34,54%	9	1	
Total			33,17%	93	7	7%

Table 3. Registered User Testing

The unregistered user identification test was conducted to evaluate the system's ability to reject access from users who have no fingerprint data stored in the database. The test involved 10 unregistered users, each performing 10 identification attempts with a confidence threshold of 50%, resulting in a total of 100 trials. Each attempt was recorded as either a correct rejection (True Negative/TN) or an incorrect acceptance (False Positive/FP), along with the average confidence score generated by the system for each unregistered user. The test results are presented in Table 3.

D. Analysis of Testing for the Registered and Unregistered User Identification System

From Table 2, testing was conducted on 10 registered users with 10 attempts each, totaling 100 trials. The system successfully recognized registered fingerprints 94 times (TP = 94) and failed 6 times (FN = 6). Several users, including Rangga Putra Aidani, Ahmad Fatih Maulana, Roma Febianti P, and Hanif Rahman, achieved perfect recognition across all attempts (TP = 10, FN = 0), while Irfan Alifiansyah recorded the highest failure rate with 2 rejections (TP = 8, FN = 2). The recognition failures were primarily attributed to wet fingerprint conditions and insufficient finger pressure during scanning, which caused unclear fingerprint patterns.

From Table 3, testing was conducted on 10 unregistered users with a confidence threshold of 50%, also totaling 100 trials. The system correctly rejected unregistered fingerprints 93 times (TN = 93) and incorrectly accepted 7 times (FP = 7). The average confidence score of 36.78%, which is below the 50% threshold, demonstrates that the system is reliable in distinguishing registered from unregistered users. Users such as Ignasius Radja N, Raka Shabran, and Yogi Yudika S were perfectly rejected (TN = 10, FP = 0), while Ikhsan Sabri and Agri Yuda each recorded 2 false acceptances (FP = 2). These false acceptances were similarly caused by wet fingerprint conditions and suboptimal finger pressure, leading the system to incorrectly identify fingerprint patterns.

E. Analysis of System Error Rates (FRR and FAR)

- False Rejection Rate (FRR)

FRR represents the system's error rate in rejecting legitimate registered users. Based on the registered user testing results in Table 2, out of 100 identification attempts by 10 registered users, the system accepted 94 times (TP = 94) and rejected 6 times (FN = 6). The FN value of 6 was accumulated from Irfan Alifiansyah B with 2 rejections, and Rizho Rahmatul, Kevin Siregar, Saskia Maharani Y, and Vira Okta F with 1 rejection each. FRR is calculated as follows:

$$FRR = (FN / (FN + TP)) \times 100\%$$
$$FRR = (6 / (6 + 94)) \times 100\%$$
$$FRR = (6 / 100) \times 100\%$$
$$FRR = 6\%$$

The results indicate that the system has a false rejection rate of 6%**,** meaning a True Acceptance Rate of 94%, demonstrating good performance in recognizing legitimate users.

- False Acceptance Rate (FRR)

FAR represents the system's error rate in accepting unauthorized unregistered users. Based on the unregistered user testing results in Table 3, out of 100 identification attempts by 10 unregistered users with a confidence threshold of 50%, the system correctly rejected 93 times (TN = 93) and incorrectly accepted 7 times (FP = 7). The FP value of 7 was accumulated from Ikhsan Sabri and Agri Yuda with 2 false acceptances each, and Ainul Yakin, Muhammad Ghazi Allawie, and Valent S with 1 false acceptance each. FAR is calculated using the following formula:

$$FAR = (FP / (FP + TN)) \times 100\%$$
$$FAR = (7 / (7 + 93)) \times 100\%$$
$$FAR = (7 / 100) \times 100\%$$
$$FAR = 7\%$$

The results show that the system has a false acceptance rate of 7% for unregistered users. In other words, the system has a true rejection rate of 93%, indicating that it is quite effective at detecting and denying access to users who do not have the necessary access rights.

F. Matrix Evaluation System

To comprehensively evaluate the performance of the fingerprint identification system, several evaluation metrics were calculated, including accuracy, precision, recall, and F1-score. Based on the data obtained from Table 5 and Table 6, the system recorded True Positive (TP) = 94, False Negative (FN) = 6, True Negative (TN) = 93, and False Positive (FP) = 7, with a total of 200 trials. These values serve as the basis for determining the system's reliability in accurately recognizing user identities.

- Accuracy measures the overall correctness of the system's classification, calculated as follows:
  Accuration = ((TP + TN) / (TP + TN + FP + FN)) × 100%
- Precision measures the system's exactness in identifying registered users from all positive predictions, calculated as follows:
  Precision = (TP / (TP + FP)) × 100%
- Recall measures the system's ability to detect all actual registered users, calculated as follows:
  Recall = (TP / (TP + FN)) × 100%
- F1-Score combines precision and recall into a single value using the harmonic mean, calculated as follows:

Class	Accuration	Presisi	Recall	F1-Score
All	94,46%	93,06%	94%	93,52%

Table 4. System Matrix Evaluation Results

Based on Table 4, the fingerprint identification system demonstrates solid and well-balanced performance with all evaluation metrics exceeding 93%. The system achieved an accuracy of 94.06%, correctly classifying 188 out of 200 total trials, supported by a Recall of 94% that minimizes false rejections against legitimate users, a Precision of 93.14% that confirms the system's exactness in validating registered users despite 7 false positive cases, and an F1-Score of 93.52% that represents the optimal balance between security and user convenience. Overall, these results demonstrate that the implemented algorithm possesses high reliability and is suitable for real-world implementation.

G. Feature Vector Results

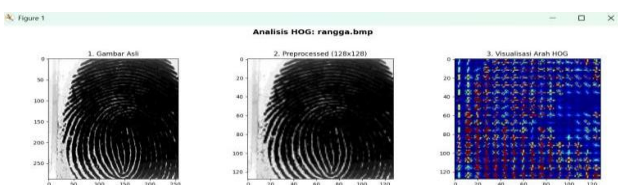


Figure 10. Results of Non Registered User Identification Testing

The feature extraction results shown in Figure 10 using the sample rangga.bmp demonstrate the effectiveness of the Histogram of Oriented Gradients (HOG) algorithm in transforming the physical characteristics of fingerprint ridges into unique and measurable numerical representations. Through the preprocessing stage, the fingerprint image was successfully standardized, enabling consistent extraction of gradient information from ridge and valley patterns. The HOG gradient direction visualization reveals the distribution of gradient angles across each image cell, representing the local structure of the fingerprint in detail. The uniqueness of Rangga Putra Aidani's fingerprint is indicated by significant feature values at the initial indices of the feature vector, such as Feature 1 (0.337559) and Feature 5 (0.156079), reflecting strong gradient intensities in specific regions of the image. This gradient value distribution pattern serves as the primary distinguishing characteristic between individuals, making the resulting HOG feature vector highly discriminative and relevant for biometric identification purposes.

The HOG feature vector is subsequently used as input to the Support Vector Machine (SVM) algorithm to determine support vectors and construct the optimal separating hyperplane between different user identities.

User	Fitur				
Rangga Putra Aidani	Fitur ke-1: 0.337559	Fitur ke-3 : 0.003619	Fitur ke-5 : 0.156079	Fitur ke-6 : 0.046971	Fitur ke-8: 0.090553
Kevin Siregar	Fitur ke-118 :0.009839	:Fitur ke-122 : 0.344357	Fitur ke-127 :0.006559	Fitur ke136 :0.350419	Fitur ke-137 : 0.350419
Irfan Alifiansyah B	Fitur ke-10 : 0.012588	Fitur ke-19 : 0.044058	Fitur ke-21 : 0.075789	Fitur ke-22 : 0.111529	: Fitur ke-23 : 0.138859
Ahmad Fatih M	Fitur ke-1 : 0.020787	Fitur ke-10 : 0.353808	Fitur ke-12 : 0.099932	Fitur ke-14 : 0.284981	Fitur ke-16 0.029397
Hanif Rahman	Fitur ke-19 : 0.081019	Fitur ke-20 : 0.236210	Fitur ke-21 : 0.028645	Fitur ke-22 : 0.045291	Fitur ke-23 0.481415
Saskia Maharani Y	Fitur ke-19 : 0.174919	Fitur ke-28 : 0.620695	Fitur ke-32 : 0.620695	Fitur ke-36 : 0.445957	: Fitur ke-55 : 0.605167
Roma Febianti P	Fitur ke-100 : 0.500000	Fitur ke-102 : 0.500000	Fitur ke-104 : 0.500000	Fitur ke 105 : 0.500000	Fitur ke118 : 0.011474
Chindy Veronica	Fitur ke-100 : 1.000000	Fitur ke-118 : 0.001993	Fitur ke-119 : 0.008915	Fitur ke120 : 0.002819	Fitur ke121 : 0.043039
Vira Okta F	Fitur ke-64 : 1.000000	Fitur ke-82 : 0.145738	Fitur ke-84 : 0.111426	Fitur ke-85 : 0.094590	Fitur ke-86 : 0.010860
Rizho Rahmatul	Fitur ke-1 : 0.058325	Fitur ke-5 : 0.099985	Fitur ke-6 : 0.009316	Fitur ke-9 : 0.038409	Fitur ke-10 : 0.516472

Table 5. Number Feature Vector Results

Each fingerprint image was processed using the Histogram of Oriented Gradients (HOG) method to extract directional and texture features. The extraction process produces a fixed-dimensional numerical vector representing the unique characteristics of ridge and valley patterns in the fingerprint, which subsequently serves as the primary input for classification using the Support Vector Machine (SVM) algorithm.

In this stage, feature extraction was performed to transform the preprocessed fingerprint images into numerical data (feature vectors) that can be processed by the SVM classification algorithm. Based on the parameters defined in the system, including an image size of 128×128 pixels, a cell size of 8×8, and 9 orientation bins, each fingerprint sample produces a high-dimensional feature vector consisting of 8,100 features. Table 9 presents a snapshot of the feature vector values from 10 sample subjects, where the displayed values represent the normalized gradient values at specific indices that characterize the unique ridge and valley patterns of each subject's fingerprint.

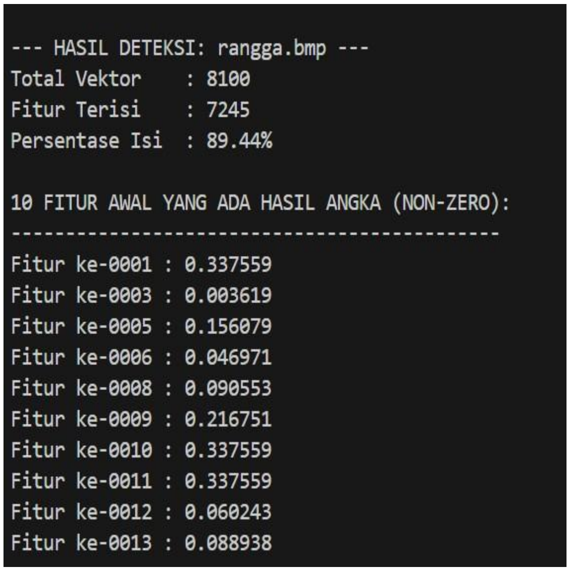


Figure 11. Stages of HOG Feature Extraction on Rangga's Fingerprint Samples

Figure 11 illustrates the fingerprint feature extraction stages of Rangga Putra Aidani using the Histogram of Oriented Gradients (HOG) method, which successfully transforms visual image information into a high-dimensional numerical representation. The process begins with image preprocessing, where the fingerprint image is standardized to 128×128 pixels to ensure uniform resolution and scale before gradient computation, thereby reducing the influence of size and finger position variations while improving feature extraction consistency. The gradient orientation visualization reveals the distribution of gradient directions and intensities across each image cell, directly representing the local structure of the fingerprint's ridge and valley patterns.

Based on the detection results, the system generates a total feature vector of 8,100 dimensions with a feature occupancy rate of 89.44%, corresponding to 7,245 non-zero features. This high occupancy rate indicates that the majority of the fingerprint image area contains relevant gradient information. The resulting numerical values, such as 0.337559 at feature index 0001, reflect strong gradient intensities at specific spatial coordinates and serve as distinctive markers of individual fingerprint patterns. The complete feature vector is subsequently stored and used as input for the SVM classification algorithm, where differences in feature value distributions between subjects enable the system to accurately and consistently distinguish user identities. Thus, the HOG feature extraction stage plays a crucial role as the primary foundation for reliable biometric identification in this study.

H. System Response Time Testing

This test was conducted to measure the system's response time from the moment the finger is placed on the fingerprint sensor until the solenoid lock physically opens. Each of the 10 registered users performed 10 identification attempts, with the solenoid configured to remain unlocked for 3 seconds upon successful verification. The average response time for each user was recorded and is presented in Table 5 below:

Pengguna	Jumlah Percobaan	Durasi Solenoid Unlock (detik)	Status Solenoid	Waktu respon rata-rata (detik)
Rangga Putra Aidani	10	3	Terbuka	8,27
Irfan Alifiansyah B			Terbuka (8x)	8,45
Rizho Rahmatul			Terbuka (9x)	8,30
Ahmad Fatih Maulana			Terbuka	8,45
Kevin Siregar			Terbuka (9x)	8,52
Saskia Maharani Y			Terbuka (9)	8,45
Roma Febianti P			Terbuka	8,54
Chindy Veronica			Terbuka	8,43
Hanif Rahman			Terbuka	8,36
Vira Okta F			Terbuka (9x)	8,51

Table 6. Number Feature Vector Results

Table 6 presents the system response time test results for unlocking the solenoid lock following a successful fingerprint identification process. The test was conducted on 10 registered users with 10 attempts each, with the solenoid unlock duration set at 3 seconds. The results show that all registered users successfully unlocked the solenoid with a "Terbuka" (Unlocked) status, with average response times ranging from 8.27 to 8.54 seconds, indicating that the system is capable of completing the entire identification and access granting process within a reasonably short time frame.

The recorded response time encompasses the entire identification pipeline, starting from fingerprint scanning by the AS608 sensor, followed by image processing using the HOG descriptor for feature extraction, and finally the classification process performed by the SVM model before sending the activation signal to the solenoid lock via GPIO. The fastest response time was recorded by Rangga Putra Aidani (8.27 seconds), while the longest was recorded by Roma Febianti P (8.54 seconds). Several users, including Saskia Maharani Y, Rizho Rahmatul, Kevin Siregar, and Vira Okta F, are indicated with (9x), and Irfan Alifiansyah with (8x), reflecting the number of successful unlock attempts out of 10 trials, which is consistent with the False Negative data previously reported in Table 5. The relatively small variation in response time across all users of approximately 0.28 seconds demonstrates the system's stable and consistent performance in executing both the fingerprint identification process and the subsequent solenoid lock activation, confirming that the system operates reliably under real-world testing conditions.

I. QR Code Scanning Test

The QR Code scanning test was conducted to ensure that the system is capable of accurately reading and processing QR Codes attached to each item as part of the identification and borrowing mechanism. This test aimed to evaluate the success of the camera or scanning device in recognizing QR Codes, as well as verifying that the data embedded within the QR Code can be correctly displayed and matched against the item data stored in the system database. The test was performed on several registered items to assess the consistency and reliability of the system under real-world usage conditions.

Figure 12. Visualization Scanning QR Code

Figure 12 illustrates the QR Code scanning process performed on an item's packaging. In this stage, the smartphone camera successfully detected and read the QR Code, subsequently displaying the IP address or borrowing system link embedded within the code. This demonstrates that the QR Code was correctly recognized by the scanning device without any reading errors, confirming the reliability of the QR Code scanning mechanism in the proposed system.

Figure 13. Result of Scanning QR Code

Figure 20 displays the borrowing system web page after the QR Code has been successfully scanned. The system automatically redirects the user to the item borrowing page, presenting the logged-in user's information along with the selected item details, such as the QR Code data and item name. The appearance of this page confirms that the integration between the QR Code and the web system is functioning correctly, and that the item data retrieved corresponds accurately to the scanned QR Code, ensuring the validity of the borrowing transaction process.

NO	Pengguna	Nama Barang	Data QR Code	Hasil Scan
1	Rangga Putra Aidani	Bor Mini	BRG001	Berhasil
2		Bor Elektrik	BRG002	Berhasil
3		HDMI Video	BRG003	Berhasil

Table 7. Result of Test Scanning QR Code

Table 7 summarizes the QR Code scanning test results for three tested items, containing information on the user name, item name, QR Code data, and scanning status. Based on the test results, all item QR Codes were successfully scanned and automatically redirected the system to the borrowing page without any errors. These results address the third research problem, namely the integration of the fingerprint identification system with digital borrowing records using QR Code, where after the user is verified through fingerprint authentication, the QR Code scanning directly records the borrowing transaction data into the database in real-time, demonstrating that the end-to-end borrowing process operates seamlessly and reliably within the proposed system.

IIII. Conclusion

Based on the results of the design, implementation, and testing conducted in this study, several conclusions can be drawn. First, the self-service borrowing system was successfully designed and implemented without the direct involvement of laboratory staff, leveraging the Raspberry Pi as the central control unit and a local database for automatic transaction recording. Second, the implementation of the fingerprint biometric method using Histogram of Oriented Gradients (HOG) feature extraction and Support Vector Machine (SVM) classification demonstrated reliable performance, achieving a model accuracy of 94.7% and an overall system testing accuracy of 94.06%. Third, the system effectively distinguished between registered and unregistered users, with a False Acceptance Rate (FAR) of 7% and a False Rejection Rate (FRR) of 6%, along with an average response time ranging from 8.27 to 8.54 seconds for the solenoid lock unlocking process, confirming that the system operates within an acceptable and consistent time frame. Furthermore, the integration of QR Code technology into the borrowing system enabled accurate item validation, where all scanned items were successfully recorded into the system database without any errors, demonstrating the reliability of the end-to-end borrowing transaction process. Overall, the developed system has been proven capable of supporting the laboratory equipment borrowing process in a self-service, secure, and well-documented manner, making it a viable solution for improving laboratory management efficiency in

References

[1] D. K. Jaya, L. E. Susilowati, and H. R. Akhdiyat, "Sistem Informasi Quick Response Code (Qr Code) Sederhana Untuk Mengoptimalkan Inventarisasi Peminjaman Dan Penggunaan Alat-Alat Laboratorium Di Jurusan Ilmu Tanah, Universitas Mataram," *Jurnal Abdi Insani*, vol. 10, no. 2, pp. 771–783, 2023, doi: 10.29303/abdiinsani.v10i2.951.

[2] G. R. Putra, B. H. Situmorang, and S. Hidayatullah, "Identifikasi Biometrika Menggunakan Ekstraksi Minutiae Pada Citra Sidik Jari," *Jurnal Teknoinfo*, vol. 17, no. 1, p. 289, 2023, doi: 10.33365/jti.v17i1.2376.

[3] F. J. Pontoh, "Teknik Deteksi Biometrika untuk Pengenalan Sidik Jari Menggunakan Deteksi Minutiae," *Pixel :Jurnal Ilmiah Komputer*

Grafis, vol. 17, no. 1, pp. 193–200, 2024, doi: 10.51903/pixel.v17i1.2000.

[4] Novita Siagian, “Perancangan Aplikasi Pengolahan Citra Digital Untuk Penajaman Sisi Citra Hasil Fingerprint Menggunakan Metode Fourier Phase Only Synthesis,” *Jurnal Ilmu Komputer, Teknologi Dan Informasi*, vol. 1, no. 2, pp. 66–75, 2023, doi: 10.62866/jurikti.v1i2.41.

[5] E. F. Laili *et al.*, “KOMPARASI ALGORITMA DECISION TREE DAN SUPPORT VECTOR MACHINE (SVM) DALAM,” *Jurnal Sistem Informasi dan Informatika (Simika)*, vol. 8, no. 1, pp. 67–76, 2025.

[6] N. Nurdiansyah, M. Muliadi, R. Herteno, D. Kartini, and I. Budiman, “Implementasi Metode Principal Component Analysis (Pca) Dan Modified K-Nearest Neighbor Pada Klasifikasi Citra Daun Tanaman Herbal,” *Jurnal Mnemonic*, vol. 7, no. 1, pp. 1–9, 2024, doi: 10.36040/mnemonic.v7i1.6664.

[7] T. Arifianto, S. Sunaryo, and L. S. Moonlight, “Penggunaan Metode Support Vector Machine (Svm) Pada,” *Jurnal Jteknik Informatika dan Teknologi Informasi*, vol. 2, no. 2, pp. 3–6, 2022.

[8] P. J. Aliffiyah and N. Pratiwi, “Deteksi Tipe Sidik Jari Untuk Mengenali Kepribadian Menggunakan Metode Support Vector Machine (SVM),” *Metik Jurnal*, vol. 9, no. 2, p. 2025, 2025, doi: 10.47002/metik.v9i2.1073.

[9] A. Zeputra and F. Utaminingrum, “Perbandingan Akurasi untuk Deteksi Pintu berbasis HOG dengan Klasifikasi SVM menggunakan Kernel Linear , Radial Basis Function dan Polinomial pada Raspberry Pi,” *... Teknologi Informasi dan Ilmu Komputer e ...*, vol. 5, no. 11, pp. 4746–4757, 2021, [Online]. Available: https://j-ptiik.ub.ac.id/index.php/jptiik/article/view/10090%0Ahttp://j-ptiik.ub.ac.id/index.php/jptiik/article/download/10090/4483

[10] A. Nishfahuddin and D. Febriawan, “Rancang Bangun Prototipe Sistem Keamanan Gerbang Rumah Otomatis Menggunakan Nodemcu ESP8266 Dengan Kendali Telegram,” *Journal of Information System Research (JOSH)*, vol. 6, no. 1, pp. 330–337, 2024, doi: 10.47065/josh.v6i1.6025.

[11] S. Purnomo and F. A. Alijoyo, “Sistem Peminjaman Barang Menggunakan QR Code Berbasis Aplikasi Android,” *Jurnal Teknologi Dan Sistem Informasi Bisnis*, vol. 6, no. 2, pp. 322–328, 2024, doi: 10.47233/jteksis.v6i2.1350.

[12] M. Bhanu Setyawan, A. F. Cobantoro, and A. Prasetyo, “Protoype Monitoring Presensi Siswa Menggunakan Finger Print Dengan Kendali Raspberry Pi,” *Jurnal Teknik Informatika*, vol. 13, no. 1, pp. 21–30, 2020, doi: 10.15408/jti.v13i1.12408.

[13] M. Faruqziddan, E. Daniati, and M. N. Muzaki, “Pendekatan BERT Dalam Analisis Sentimen Terhadap Kominfo Di Media Sosial X,” *The Indonesian Journal of Computer Science Research*, vol. 4, no. 2 SE-Articles, pp. 107–116, 2025, [Online]. Available: https://subset.id/index.php/IJCSR/article/view/207

[14] F. Putrawansyah, “Penerapan Metode Support Vector Machine Terhadap Klasifikasi Jenis Jambu Biji,” *JIKO (Jurnal Informatika dan Komputer)*, vol. 8, no. 1, p. 193, 2024, doi: 10.26798/jiko.v8i1.988.

[15] A. Choerudin, J. Windarta, and Sumardi, “Perancangan sistem informasi peminjaman alat dan peralatan laboratorium berbasis RFID,” *Journal of Telecommunication, Electronics, and Control Engineering (JTECE)*, vol. 3, no. 1, pp. 41–47, Jan. 2021.