Jurnal Rekayasa Elektrika Vol. 21, No. 2, June 2025, page 93-103
ISSN. 1412-4785; e-ISSN. 2252-620X, Accredited by Kemendikbudristek No. 105/E/KPT/2022
DOI: 10.17529/jre.v21i2.41142

Authentication of an Indonesian ID Card with Simultaneous NFC and Face Recognition

Chairullah Chairullah*, Yuwaldi Away, and Maulisa Oktiana
Department of Electrical and Computer Engineering, Universitas Syiah Kuala
Syech Abdurrauf str., No. 7, Darussalam, Banda Aceh, Aceh 23111
*e-mail: chairullah@mhs.usk.ac.id

Abstract—**Identity (ID) card forgery remains a significant issue in Indonesia, often leading to crimes such as identity theft and fraud. To address this challenge, this study proposes the development of an identity authentication system that integrates near field communication (NFC) and facial recognition based on K-nearest neighbors (KNN) algorithm. The primary objective of this system is to enhance the security of ID card (KTP) data and to ensure efficient and accurate access to services requiring identity verification. The system stores facial data and ID card information securely in Firebase, which serves both as a user authentication platform and a secure cloud-based storage solution. The application, developed using Flutter, incorporates facial recognition for biometric verification, while NFC is employed as an additional authentication layer to provide dual-factor verification and reinforce identity security. Experimental results demonstrate that the facial recognition based on KKN achieved an accuracy rate of 100% with a false acceptance rate (FAR) of 0%, indicating a highly reliable performance. These findings confirm that the integration of facial recognition and NFC technologies offers a robust and effective solution to combat ID card forgery, thereby improving the overall reliability and security of the population data authentication system in Indonesia.**

Keywords: ***authentication, face recognition, ID card, knn, nfc***

I. Introduction

The current development of identity documentation in Indonesia is reflected in the implementation of the electronic identity (ID) card system, known as the e-KTP. This system is designed with both physical and digital components to enhance administrative efficiency and data accuracy. The e-KTP program was officially launched by the Ministry of Home Affairs of the Republic of Indonesia in February 2011. Following Law number 24 of 2013, which amends Law number 23 of 2006, it is mandated that each citizen may possess only one ID card containing a unique National ID Number (NIK), which serves as a lifelong personal identifier [1].

Despite the implementation of the e-KTP system, significant challenges remain, particularly with regard to ID card forgery across various regions in Indonesia. The falsification of population data is among the most prevalent forms of crime in the country and remains difficult to eradicate. Such fraudulent activities are often exploited for various unlawful purposes, including identity theft, financial fraud, and unauthorized access to government services [2]. Previous research conducted by Norma et al. focused on the completeness of data and information in the e-KTP system by optimizing biometric technology [3]. However, the scope of this study was limited to verifying individual identity information without addressing the broader issue of document authenticity and security.

Fingerprint recognition is considered one of the most accurate and reliable biometric technologies for identity verification. As the misuse and vulnerability of conventional security mechanisms such as passwords and personal identification numbers (PINs) continue to rise, biometric systems have emerged as a more secure alternative by utilizing the unique physiological or behavioral characteristics of individuals [4]. Biometric identification can be implemented through unimodal systems, which rely on a single biometric trait, or multimodal systems, which combine multiple traits for enhanced performance. However, unimodal systems such as those based solely on fingerprints are prone to several limitations, including sensor noise, lack of universality (i.e., not all users can provide usable data), and susceptibility to spoofing or forgery attempts [5].

In response to the growing threat of ID card forgery, this research proposes an innovative approach to enhancing ID card security by integrating near field communication (NFC) and facial recognition technologies. NFC is a hardware component commonly embedded in smartphones that enables short-range wireless communication between compatible devices via radio frequency within a limited distance [6]. In contrast, facial recognition is a biometric technology capable of identifying and verifying individuals by analyzing and comparing facial features captured through a camera. The system utilizes pre-stored facial data within a dataset and is commonly implemented

Received 4 Nov. 2024; Revised 8 May 2025; Accepted 2 June. 2025

in security systems as an access control mechanism [7]. This technology enables the system to accurately interpret and distinguish individual facial characteristics. Specifically, facial landmark data extracted from images are transformed into numerical vectors or mathematical representations, each uniquely corresponding to a specific face [8].

The proposed method has the potential to enhance identity security by implementing an authentication system based on civil registration data, thereby ensuring that the individual presenting the ID card is its legitimate owner. In this system, facial data and user ID card information are uploaded to Firebase, a platform that offers robust user authentication services and secure cloud-based data storage. Firebase serves as an effective solution for managing and safeguarding identity-related data and facial recognition outputs, offering rapid accessibility and high reliability. Its strong security architecture and scalability make it particularly suitable for handling sensitive and large-scale identity data [7]. Additionally, the use of Flutter facilitates efficient development and seamless integration of complex functionalities, such as camera access and facial recognition result visualization, within the ID card application.

Users can utilize their personal mobile devices to access the application, which allows them to capture facial images that serve as input for the face recognition process [9]. The results of this recognition are then transmitted to Firebase in the form of corresponding ID card (e-KTP) data. The Flutter-based application retrieves this information from Firebase and presents it in the form of user photographs and identity details. The development of this system offers a promising solution to combat ID card forgery, enhance security, and ensure efficient and accurate access to services requiring identity verification.

The main contributions of this research are as follows:

1. Development of a population data matching model based on the integration of NFC and facial recognition based on K-nearest neighbors (KNN) algorithm.
2. Prototype testing of an identity authentication system in the form of a mobile application that integrates both NFC and face recognition capabilities.

II. Method

A. Material

The materials utilized in this study consist of facial image datasets and ID card holder data, which were collected with prior consent and approval by ethical standards. The data collection process follows the workflow illustrated in Figure 1. The facial recognition process in this study relies on identifying unique facial landmarks extracted from individual facial features. The dataset employed includes 129 electronic ID cards (e-KTP) with a resolution of 480×600 pixels, obtained from the Directorate General of Population and Civil Registration Office of Great Aceh Regency, with prior permission and ethical approval. Each data entry is accompanied by corresponding identity information—such as name, NIK, address, and other relevant attributes—and is securely stored in Firebase.

The development and implementation of the system utilize several software tools, including Python (managed through Anaconda), Visual Studio Code, and Flutter for mobile application development. Additionally, testing was conducted using smartphones equipped with NFC functionality to support the ID card authentication process.

B. Identity Authentication Scheme

The steps to create a population identity authentication system are as shown in Figure 2. In this research, the face recognition model and KNN are used and the application

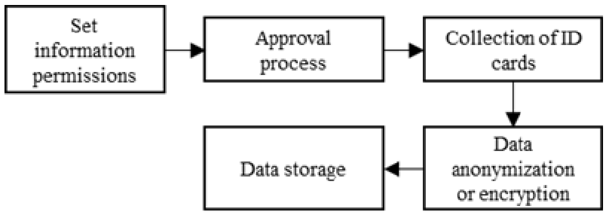


Figure 1. Flowchart collection ID card

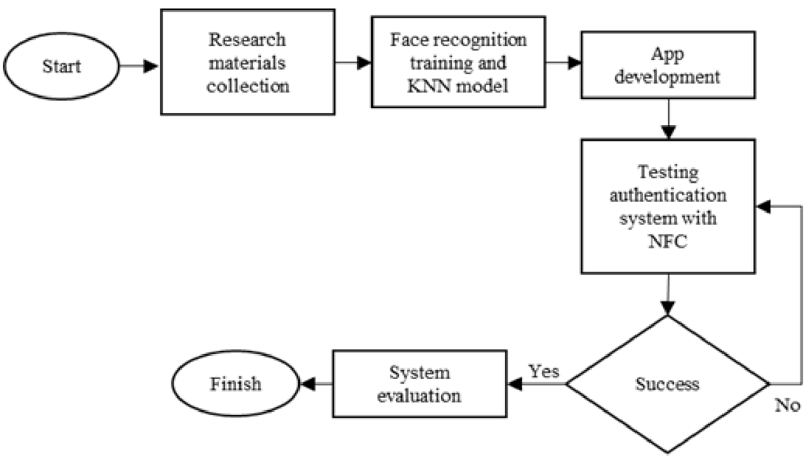


Figure 2. Schematic of ID authentication system

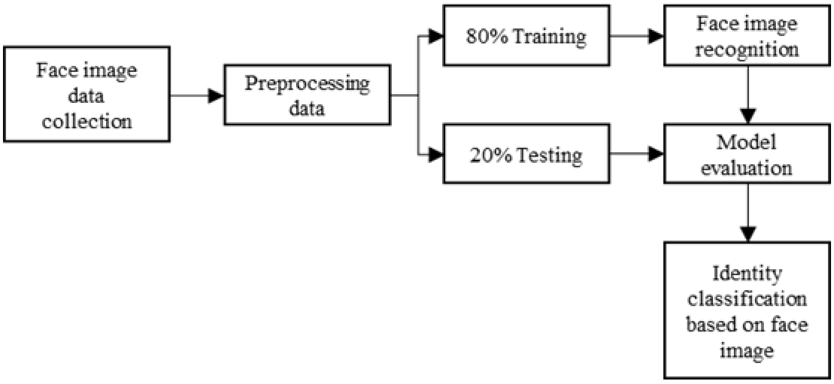


Figure 3. The identity data classification process based on facial images

is built. The selection of the KNN model is based on the characteristics of a small and homogeneous dataset, where the complexity of models such as convolutional neural network (CNN) has the potential to cause overfitting.

Furthermore, the choice of the KNN algorithm is motivated by the limitations in computational resources and the need to maintain model transparency. While CNNs generally exhibit superior performance in large-scale and complex recognition tasks, KNN provides an optimal trade-off between accuracy, computational efficiency, and interpretability within the scope of this study. Facial recognition is employed as the core of the security system due to its non-intrusive nature, as it does not require direct physical contact with biometric sensors—unlike other biometric authentication methods [10].

Facial recognition technology has evolved significantly, expanding its applications beyond traditional computer systems to include mobile platforms and robotics [11]. In the recognition process, key facial features such as the nose, eyes, and lips are analyzed to enable accurate identification [12]. Generally, face recognition systems are categorized into two types: image-based systems, which focus on static physical appearance, and video-based systems, which account for dynamic changes in appearance over time, such as facial expressions or head movements [13].

This study focuses on a facial recognition method that employs the KNN algorithm for classification. The application is integrated with the NFC feature available on smartphones, enabling a dual-layered identity verification process through data matching. NFC technology utilizes electromagnetic induction and standardized communication protocols to enable fast, secure, and short-range data transmission between nearby devices [14]. The integration of NFC in this system enhances the robustness of identity verification and contributes to the mitigation of ID card forgery, thereby strengthening the security of personal identity data.

C. Train Face Recognition and KNN Model

At this stage, the facial recognition model is trained using pre-collected e-KTP photographs. The objective of this training process is to enable the application to accurately recognize and match the facial image of the ID card holder. The classification process utilizes the KNN algorithm, as illustrated in Figure 3. KNN is a supervised machine learning algorithm commonly applied in classification tasks, including facial recognition [15]. The algorithm determines the identity of an input face by comparing it to the *K* nearest neighbors in the dataset, using Euclidean distance as the similarity metric [16].

The research stages begin with the collection of 129 facial image data, followed by a preprocessing phase to enhance data quality and consistency. The dataset is then divided into two subsets, comprising 80% for training and 20% for testing. The training phase involves building the face recognition model, while the testing phase is conducted to evaluate the model's ability to accurately predict and recognize individual identities based on input facial images. The KNN algorithm is employed for this classification task, as outlined in Algorithm 1, to assess its effectiveness in identifying population identities through facial recognition.

Algorithm 1. Train KNN

Input: face images
n_neighbors: 2
KNN algoritma: 'ball_tree'

Output: KNN_model

for all face image do
I_m ← face image
I_e ← apply face encoding to I_m
X, Y ← save face encoding I_e and image name to list
end for
KNN_cls ← declares model KNN
KNN_cls ← train using (X, Y)
Save model
Return model

D. Authentication Application

In this phase, the application is developed using the Flutter framework, with Firebase utilized for data storage, a facial recognition model for detecting and identifying faces, and NFC functionality on Android devices for

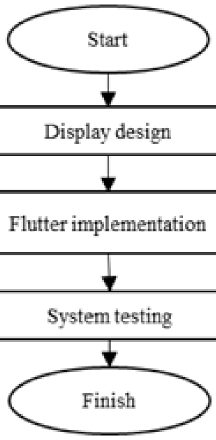


Figure 4. System development flow

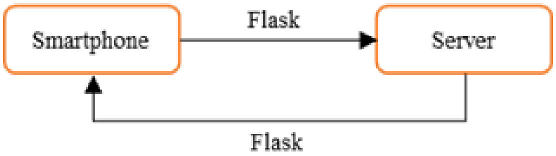


Figure 5. Illustration of system performance

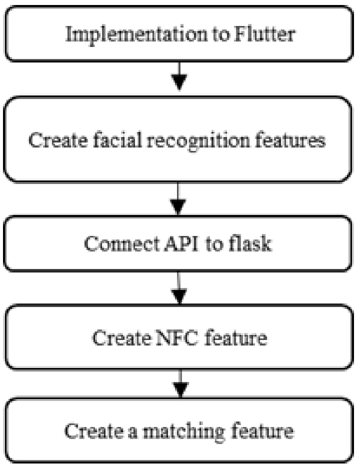


Figure 6. Testing the application working system

accurate tracking and authentication of resident data. Flutter is a cross-platform mobile development framework that uses the Dart programming language to build applications for both Android and iOS platforms [17]. This framework allows for high-performance execution by compiling Dart code into native code, and it supports dynamic interaction by enabling the reading and modification of widget states throughout the application lifecycle [18], [19].

The complete system workflow is presented in Figure 4. ID card (e-KTP) data is securely stored in a pre-configured Firebase database, ensuring reliable access and protection of sensitive information. The collection, storage, and utilization of e-KTP data adhere to applicable data protection regulations and ethical standards, requiring prior informed consent from the individuals concerned or formal authorization from the Directorate General of Population and Civil Registration.

Firebase is a cloud-based platform that offers comprehensive backend services to support the development of iOS, Android, and web applications [20]. Through features such as the Realtime Database and Cloud Firestore, Firebase facilitates real-time and offline data synchronization, monitoring, and support for client-side applications [21], [22]. In this study, the e-KTP data stored in Firebase includes personal information such as the holder's name, NIK, address, facial image, and other relevant attributes. A pre-trained face recognition model is prepared and integrated into the system. This model is then connected with both the NFC functionality and the Flutter-based application to enable seamless identity verification. The integration ensures that user authentication is conducted accurately and securely within a single application environment.

Table 1. Data split

Type of data	Training	Testing
e-KTP	103	26
Facial images	1227	327

E. Testing the Authentication System with NFC

The authentication system testing using NFC is conducted with a smartphone equipped with NFC capability and connected to a data server via the Flask framework. In this configuration, devices can operate either as NFC readers or tags, enabling data exchange through short-range communication. NFC technology facilitates seamless information transfer, allowing users to perform tasks such as bill payments, exchanging digital contact information, or downloading promotional content with a simple touch [23]. In the context of this study, the ID card is brought into proximity with the smartphone running the authentication application, initiating the identity verification process through secure and contactless data transfer.

The application was developed using the Flutter framework, and system testing was conducted as illustrated in Figure 5. The testing procedure begins with capturing a real-time facial image of the ID card holder using a smartphone camera through the Flutter-based application. The system then performs facial recognition and displays the predicted results, which include the e-KTP holder's face image, name, NIK, address, and other relevant personal information. The output of the face-matching process is presented in Figure 6, demonstrating the application's ability to retrieve and display the corresponding identity data based on the input facial image.

Subsequently, the NFC module is used to validate the results obtained from the facial recognition process, thereby minimizing the risk of e-KTP forgery. The NFC card contains embedded information such as the holder's facial image, name, NIK, address, and other identity details. Based on the outcome of both the facial recognition and NFC verification processes, the system determines whether the user is granted access. If both authentication mechanisms return matching and valid results, the identity

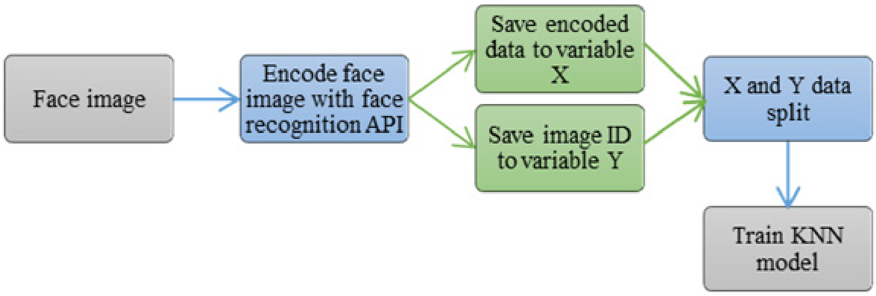


Figure 7. Face recognition model testing

Table 2. Labelling of face image ID

No.	ID of facial images	No.	ID of facial images
1	8002288495444000	16	800E153108247134
2	800248C316444000	17	800E173D08247134
3	8002546F2E444000	18	800E184C11882D33
4	80025472AE444000	19	800E203D08247134
5	80025761AE444000	20	800E221B14111134
6	80046C90B2456080	21	800E2518146CCF33
7	800580CCDD41D100	22	800E2741027F2F33
8	8005817EE51D1300	23	800E294901247134
9	80058E229B0DF200	24	800E2A4901247134
10	80058F69D8817200	25	800E2E3D08247134
11	800E0C3D08247134	26	800E2F4901247134
12	800E0D4501247134	27	800E304901247134
13	800E0E4501247134	28	800E334901247134
14	800E0F1C08247134	29	800E4F4C1828D334
15	800E101B14111134	30	80188235E17C3E8C

is confirmed, and access is authorized. Conversely, if either verification fails, the system prompts the user to repeat the verification process or initiates additional identity confirmation procedures to ensure authenticity.

III. Result and Discussion

A. Dataset Processing

The initial stage in the development of a population identity authentication system utilizing NFC and facial recognition involves dataset processing. This process begins with data acquisition, where facial images are captured using a smartphone to serve as biometric identifiers for population identity. The extracted facial features are then systematically organized and assigned a unique identifier (face ID), which is used to link each face to the corresponding ID card data. The ID card dataset comprises personal information such as the individual's name, address, date of birth, and NIK. The system is also tested under scenarios in which facial recognition may encounter difficulties in accurately labelling or matching an individual's identity with their ID card information. To ensure data privacy and security, the unique face ID functions as a secure key to access and retrieve the associated identity record from the database.

All data are stored in a secure database equipped with encryption mechanisms to ensure the protection of sensitive personal information. The dataset used in this study consists of 129 ID card entries and 1,554 facial images, which are divided into 80% for training and 20% for testing, as presented in Table 1. In this dataset, each individual is treated as a distinct class, resulting in several classes equivalent to the number of unique persons. This class-based division enables the system to accurately recognize individuals by leveraging distinctive facial features and subsequently linking them to their corresponding ID card records. Table 2 illustrates an example of labelling involving 30 identity records, which includes NIK and corresponding facial data, serving as the ground truth for system evaluation and training.

B. Face Recognition Model

The system was trained using a dataset comprising facial images that had been previously labelled with the corresponding identity information, as illustrated in Figure 7. These facial images, collected from various individuals, were systematically linked to ID card data using a unique identifier (face ID), as detailed in Table 1. During preprocessing, the facial images were analyzed to extract distinctive biometric features. This process utilized a face recognition API to encode each image into a numerical representation based on key facial landmarks. Unique characteristics such as the distance between the eyes, the contour of the nose, and overall facial geometry were extracted to distinguish one individual from another with high accuracy.

The encoded facial data are reduced into a fixed-length feature vector of 128×1 dimensions and subsequently stored in the variable X, representing the input features. Correspondingly, the associated identity labels, derived from the ID card data, are stored in the variable Y, representing the target output. Each encoding in X is uniquely linked to a user ID in Y, enabling supervised learning. This structured dataset is then used to train the KNN model, as outlined in Table 2. The training process allows the model to learn the distinctive facial features represented in X and to associate them accurately with the corresponding user identities in Y, thereby enabling effective recognition and classification of individual faces based on their biometric signatures.

In the KNN model applied for face recognition, a

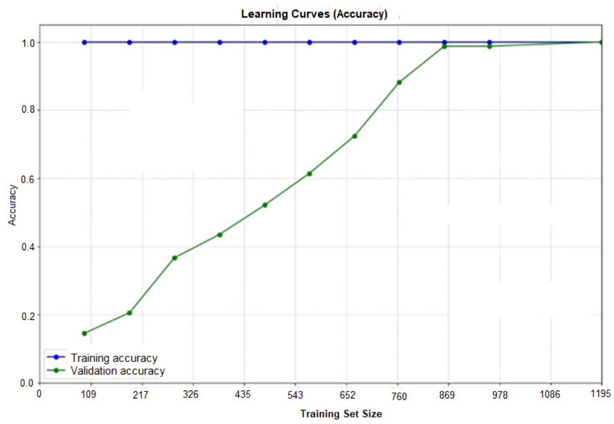


Figure 8. Model training and validation results

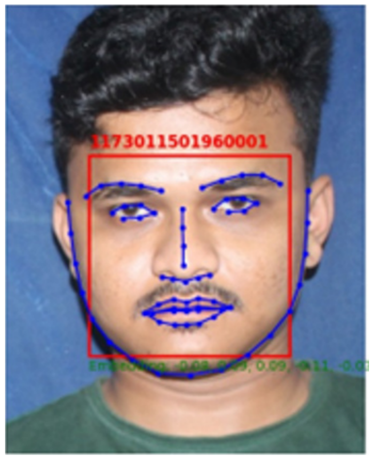


Figure 9. Face recognition results based on ID

clustering-based approach is employed to identify and classify individual identities based on facial feature similarities. A key hyperparameter in the model is "n_ neighbors", which determines the number of nearest neighbors considered during the classification process. In this study, the optimal value for "n_neighbors" was selected based on preliminary experimentation or approximated using the square root of the total number of training samples, as commonly recommended in KNN implementations. To efficiently search for the nearest neighbors, the "ball_tree" algorithm is utilized due to its effectiveness in handling high-dimensional data such as face embeddings. Furthermore, the weights parameter is set to "distance" to assign greater influence to closer neighbors during prediction. This weighting scheme enhances the model's discriminative ability by prioritizing more similar facial vectors, thereby improving the accuracy of identity classification.

In this study, a distance threshold is implemented to determine the similarity level required for a new facial input to be considered a match with the existing training data. This threshold plays a crucial role in minimizing the risk of misidentification by defining a decision boundary for classification. If the Euclidean distance between the encoded features of a newly captured face and those stored in the training set falls below the predefined threshold, the system recognizes the input as belonging to a specific individual. To evaluate the effectiveness and reliability of the face recognition system under practical conditions, comprehensive model testing was conducted. This assessment measured the model's ability to accurately identify individuals based on facial features. The performance results of the face recognition model using the KNN classification method are illustrated in Figure 8.

The analysis of the learning curve derived from the training dataset indicates that the training accuracy rapidly stabilizes at a value of 1.0, reflecting perfect performance on the training data. Conversely, the validation accuracy exhibits a notable increase starting from the 109th data point, continuing to improve until it reaches 1.0 around the 800th sample. From the 800th to the 1200th data point, both training and validation curves begin to converge, with the validation accuracy ultimately reaching 1.0 near the 1000th data point. These results suggest a potential issue of overfitting, where the model demonstrates exceptionally high accuracy on the training data while initially struggling to generalize to unseen validation data. Although the validation accuracy eventually reaches parity with the training accuracy, the early gap between the two curves highlights the model's tendency to memorize the training data rather than generalize well. This condition warrants further investigation, such as through cross-validation or the application of regularization techniques, to ensure robust model performance in real-world scenarios.

C. Face Recognition Results

The face recognition model that has been built using the KNN method is then tested using data that has been given an ID based on the NIK e-KTP. The data that has been labeled is ID and NIK based on face and identity data as shown in Table 2. As shown in Table 1, At the stage of encoding facial images for identity authentication based on the NIK e-KTP, ID labeling is carried out by associating the results of facial image encoding with the owner's NIK. The process begins with capturing an image of a person's face using a camera, which is then processed using the face recognition API to produce encoding in the form of vectors that represent the unique features of the face.

Subsequently, the encoded facial image data are stored in a designated variable (commonly referred to as X), while the corresponding NIK from the ID card is stored in a separate variable (Y) as a unique label representing each individual's identity. By assigning the NIK as the label for each encoded vector, the system ensures a direct and accurate mapping between the biometric data and the official population identity. This linkage facilitates seamless integration with external systems that rely on the NIK as a primary identifier and enhances overall security by supporting robust and precise identity authentication mechanisms. The workflow of this process is illustrated in Figure 9.

Three examples of facial recognition results using the KNN-based face recognition method are presented. In each instance, the detected face is enclosed within a

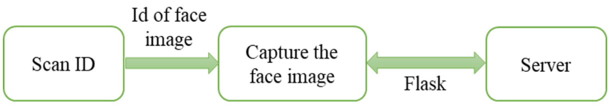


Figure 10. Flow of the ID authentication system using NFC

red bounding box, which denotes the area identified by the system as containing a face. Within these bounding boxes, blue lines indicate facial landmark points such as the positions of the eyes, nose, and mouth. These landmark points are critical in aiding the facial recognition algorithm to extract and analyze the distinctive features of each individual, thereby enabling accurate identity classification.

At the top of each red bounding box, a unique identification number (e.g., “1173011501960001”) is displayed, representing the individual ID assigned through the facial authentication process. This ID is derived from the NIK associated with the facial image. Additionally, at the bottom of each image, an embedding value is shown, which refers to a numerical vector encoding the unique facial features. These embeddings are utilized by the KNN algorithm to calculate the Euclidean distance between the input facial features and those stored in the reference database, enabling accurate identity matching and classification.

The KNN method operates by identifying the nearest neighbor within a feature space defined by facial embedding vectors. When a new face embedding is evaluated, its Euclidean distance is calculated against the embeddings stored from the training data. If the closest match corresponds to a particular ID, the system recognizes the face as belonging to the individual associated with that ID. This mechanism enables the system to automatically and efficiently authenticate a person’s identity. Furthermore, when integrated with NFC technology, this approach enhances the reliability of the authentication process by combining biometric verification with secure digital identity data, thereby reinforcing overall system security.

By employing this dual-factor approach, the system is capable of accurately validating an individual’s identity using both NFC data (e.g., from an electronic ID card) and facial data captured via a camera. The application of the KNN algorithm in facial recognition demonstrates its effectiveness in mapping facial images to unique identifiers. This capability is particularly significant in the context of security systems and population identity authentication, where accurate and reliable verification is essential to prevent identity fraud and ensure data integrity.

D. Application System Testing

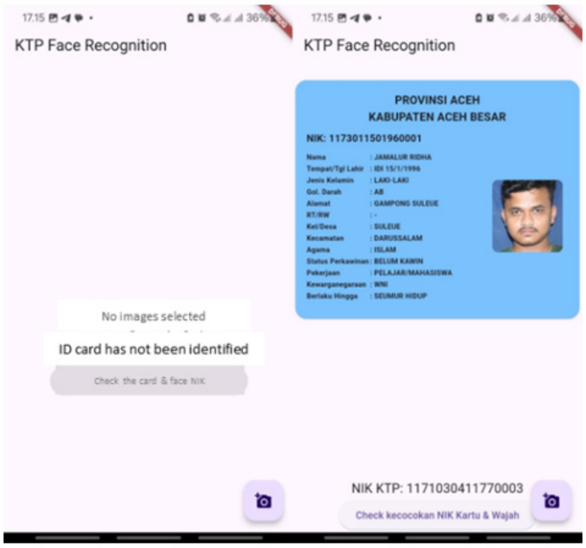
The system architecture that integrates NFC and face recognition technologies offers a robust and efficient solution for identity authentication. By employing carefully selected hyperparameters within the KNN model, the system demonstrates a high level of accuracy under real-world conditions. This study has elaborated on the key components of the system, detailed their respective functions, and highlighted the critical role of hyperparameter tuning in optimizing the performance of the face recognition process. The combination of biometric and digital verification methods enhances the security, reliability, and scalability of the identity authentication system.

This study evaluated the ID authentication system by testing its integrated face recognition and NFC-based ID scanning functionalities within the developed application. The testing workflow, as illustrated in Figure 10, begins with capturing a facial image using the smartphone’s camera. The captured image is then uploaded to Firebase, which facilitates ID scanning by referencing a pre-trained dataset. Subsequently, the associated ID data is transmitted to the server via a Flask endpoint (credit) to extract facial features and perform a matching process against the stored ID records. The server receives a request from the smartphone application containing both the facial image and the corresponding ID data, enabling the system to validate the individual’s identity.

The server processes the received facial image by extracting its unique features and matching them with the corresponding ID data. The face recognition model is executed on the server to determine whether the uploaded facial image corresponds to the identity data retrieved through the prior ID scan. Upon completing the recognition process, the Flask endpoint returns a response indicating whether the user’s facial identity matches the scanned ID data. This integrated system, which combines NFC-based ID scanning with face recognition, aims to ensure that the individual’s facial characteristics are consistent with their official residency data, thereby enhancing the security and reliability of the identity authentication process.

The application developed, as illustrated in Figure 11(a), features an integrated camera module for capturing facial images. Users can upload facial images directly through a device connected to the system. Once the image is processed, the application displays the corresponding identity details based on the ID data that matches the recognized facial features, as shown in Figure 11(b). To enhance verification, users are instructed to bring their ID card close to a smartphone equipped with NFC capabilities. This NFC interaction enables the application to scan the identity data embedded in the electronic ID card (e-KTP), thereby facilitating the matching process between the scanned ID data and the actual personal identity stored in the system.

To display the results of residency identity verification, the system employs a face recognition algorithm to extract facial features from the uploaded image and identify the corresponding face ID within the database. Once the face ID is successfully recognized, the system retrieves associated identity data, including the NIK, from the database. Simultaneously, data extracted from the NFC chip embedded in the ID card is verified against the facial recognition results to ensure the accuracy of identity authentication. If the NFC data matches the facial recognition data, the system confirms the validity of the



(a) (b)

Figure 11. Application results for identity authentication

identity and associates it with the correct NIK. Conversely, if a mismatch is detected between the NFC data and the facial recognition output, the system will notify the user that the identity verification has failed due to inconsistencies in the data. The corresponding notification display is illustrated in Figure 12.

E. Analysis and Evaluation System

The confusion matrix is used to evaluate the performance of classification models. In binary classification tasks, the confusion matrix consists of four components such as [15]

- True Positive (TP) indicates the number of positive instances that are correctly predicted by the classifier.
- True Negative (TN) represents the number of negative instances that are correctly classified.
- False Positive (FP) refers to negative instances that are incorrectly predicted as positive.
- False Negative (FN) denotes positive instances that are incorrectly classified as negative.

This matrix allows for a detailed analysis of classification errors and provides insight into the types of misclassifications made by the model. Based on the confusion matrix, several performance metrics can be derived, including accuracy, recall, precision, and the F1-Score, which are commonly used to assess the effectiveness and robustness of classification models [24].

The final stage after training and testing the face recognition model using the KNN algorithm and integrating it with NFC technology is system analysis and evaluation. The evaluation results are illustrated through a confusion matrix, as shown in Figure 13. The confusion matrix provides a visual representation of the classification model's performance by showing the correlation between actual labels and the model's predictions. The values located along the main diagonal (from the top-left to the

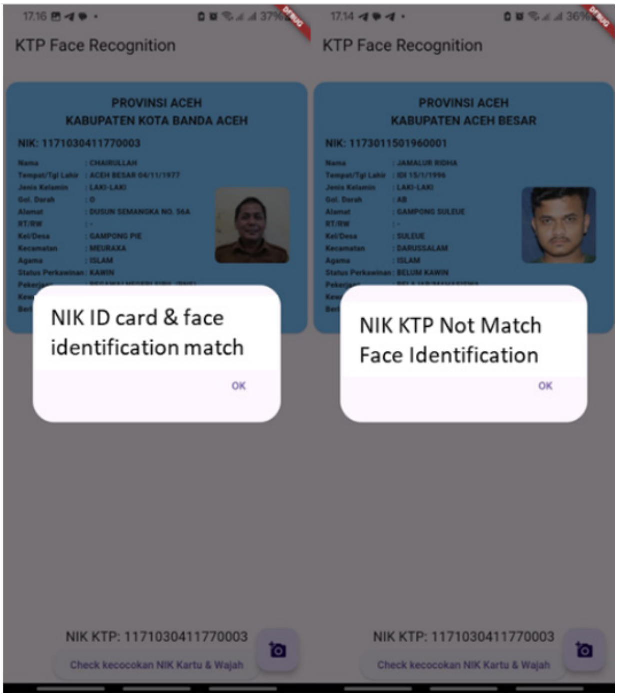


Figure 12. Matching method result

bottom-right) represent the number of correctly classified instances for each class. In contrast, values outside the main diagonal indicate misclassifications made by the model. The accuracy of a multi-class classification model can be inferred by the concentration of values along the diagonal [25]. The fewer the off-diagonal values, the better the classification performance. As depicted in Figure 13, most of the values are concentrated on the main diagonal, suggesting that the model demonstrates strong performance in recognizing and classifying facial images accurately across multiple identity classes.

Furthermore, nearly all values outside the main diagonal are zero, indicating that the model makes very few classification errors. This suggests that the system is highly precise in matching facial images to the correct identity class. The confusion matrix consists of numerous classes, as indicated by the labels on both the X and Y axes, which represent unique identification numbers derived from NFC and face recognition data. The high values along the main diagonal for specific IDs—such as "1171091008060001" and "1171030411770003"—demonstrate that the model performs exceptionally well in correctly classifying these individual identities. This pattern suggests strong discriminative capability of the model in recognizing facial features and associating them with the correct identity labels across a multi-class classification problem.

Based on Figure 13, the values of precision, recall, F1-score, and accuracy can be calculated using the calculations in (1) to (4). The values of TP, TN, FP, and FN are shown in Table 3. TP indicates the number of samples that are truly positive and predicted positive by the model, TN is the number of samples that are truly negative and predicted negative by the model, FP is the number of samples that

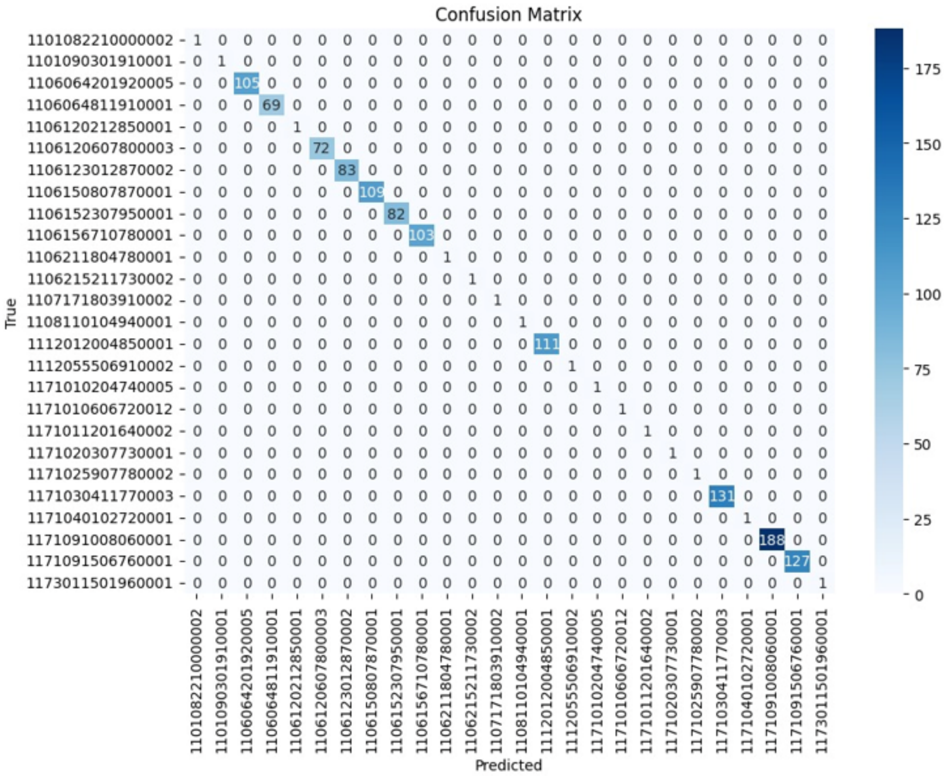


Figure 13. Confusion matrix result

Table 3. Component value of the confusion matrix

	Actual Value	
Predicted Value	1203	0
	0	0

are truly negative but predicted positive by the model, and FN indicates the number of samples that are truly positive but predicted negative by the model.

$$\text{Accuracy} = \frac{\text{TP}+\text{TN}}{\text{TP}+\text{FP}+\text{TN}+\text{FN}} \times 100\% \qquad (1)$$
$$= \frac{1203}{1203} \times 100\% = 100\%$$

$$\text{Precission} = \frac{\text{TP}}{\text{TP}+\text{FP}} \times 100\% \qquad (2)$$
$$= \frac{1203}{1203} \times 100\% = 100\%$$

$$\text{Recall} = \frac{\text{TP}}{\text{TP}+\text{FN}} \times 100\% \qquad (3)$$
$$= \frac{1203}{1203} \times 100\% = 100\%$$

$$\text{F1-score} = 2 \times \frac{\text{Precission} \times \text{Recall}}{\text{Precission} + \text{Recall}} \qquad (4)$$
$$= 2 \times \frac{10{,}000}{200} = 100$$

$$FAR = \frac{FP}{TP+FP} \times 100\% \qquad (5)$$
$$= \frac{0}{1203} \times 100\% = 0\%.$$

Furthermore, based on data from NFC and face recognition, a false acceptance rate (FAR) calculation is needed to evaluate the population identity authentication system. The application is tested by matching real-time facial images with a user database [24]. In biometric systems, access errors by unauthorized users are measured as FAR. The lower the FAR, the better the system prevents unauthorized access [5]. This calculation is used in evaluating the matching method, which in this study matches biometric data in the form of face images and ID cards. The FAR calculation value refers to Figure 13 and is calculated using (5). The results of the FAR calculation show that the percentage error of this system is 0%, this shows that the proposed method is successful in doing well in securing identity.

Based on the results obtained in this study, a comparison has been made with several related previous works. These comparisons serve to highlight the improvements and validate the effectiveness of the proposed system. Previous studies have focused on the development of biometric systems, particularly in facial recognition using various approaches and algorithms. Table 4 presents a comparative analysis of the current research outcomes with those from prior studies, demonstrating that the system developed in this study has achieved superior or comparable performance. This indicates the success and relevance of the integration between NFC and face recognition for

Table 4. Comparison of methods

No.	Method	Accuracy
1	Face recognition + KNN [5]	95%
2	Face recognition + CNN + NFC [6]	95%
3	Face recognition + CNN [7]	98%
4	**NFC + face recognition based on KNN**	100%

secure identity authentication.

It can be concluded that the integration of NFC and face recognition using the KNN method demonstrates superior performance in the development of a resident identity authentication system. Previous research employing CNN and NFC for face recognition reported an accuracy of approximately 95%. In contrast, the proposed system using the KNN algorithm combined with NFC achieved an accuracy rate of 100% during testing. These findings indicate that the method presented in this study outperforms previous approaches and supports the conclusion that the proposed system is effective and successful in accurately authenticating population identity.

The KNN can outperform CNNs in NFC-based population identity authentication involving facial image recognition for several technical reasons. Firstly, KNN is a non-parametric and straightforward algorithm that classifies input data by calculating the distance between the input and stored reference data, assigning the label based on the majority class among the nearest neighbors. This simplicity allows KNN to be effectively applied in systems with limited computational resources and small datasets. In contrast, CNNs typically require large-scale training data and extensive computational resources to achieve optimal performance. Consequently, in scenarios where training data is limited such as in population authentication systems with a relatively small number of facial images—KNN may offer better efficiency and accuracy compared to CNNs.

In addition, KNN offers greater computational efficiency and lower latency compared to CNNs, as it does not require an intensive training phase. Instead, KNN simply calculates the distance between input data and stored samples during inference. Conversely, CNNs demand substantial computational resources, particularly for training, as they rely on optimizing numerous parameters over multiple epochs. Within the context of NFC-based identity authentication using facial imagery, KNN enables quicker deployment and simpler face-matching mechanisms, making it more feasible for lightweight or real-time applications, whereas CNNs may be overly complex and typically require specialized hardware (e.g., GPUs or TPUs).

Moreover, KNN tends to be more resistant to overfitting in small or finite datasets, given that it lacks a parameterized training phase. This characteristic enhances its reliability when the available training data is limited. Its non-parametric nature makes it especially suitable for implementation in embedded systems or edge devices where computational power and memory are constrained. Therefore, in NFC-based identity verification systems involving facial recognition, KNN can serve as a more practical and efficient solution, particularly when the data is small-scale, low-dimensional, or already pre-processed. However, for applications requiring the extraction of complex patterns or handling large-scale datasets, CNNs may still be the preferred method, provided that adequate computational resources are available.

IV. Conclusion

Based on the research conducted on the development of a population identity authentication system utilizing NFC and face recognition, it can be concluded that the integration of these two technologies represents a promising innovation for enhancing identity verification and preventing forgery. The combined NFC and face recognition model outperforms other comparative methods in terms of accuracy and reliability. The matching mechanism, which compares facial image data and NIK stored in Firebase, has proven effective in addressing the issue of ID card forgery. This is supported by the results of the confusion matrix analysis, which demonstrate an accuracy rate of 100% and a FAR of 0%. Although these results appear ideal, it is important to note that such performance metrics require further validation using more extensive and diverse datasets, as well as real-world implementation scenarios. Future studies are encouraged to explore the system's generalizability by incorporating larger datasets, refining model architectures, and applying regularization techniques to address potential overfitting issues observed during training.

References

[1] M. F. Faisal, "Analisis tindak pidana pemalsuan e-KTP abstrak," *Jurnal Kajian Hukum*, vol. 3, no. 2, pp. 94-10, 2022.

[2] C. Andika, M. Inacio, and W. S. Nugroho, "Law enforcement of population data manipulation in Malaka district," *Jurnal Lawnesia*, vol. 1, no. 2, pp. 136-142, 2022.

[3] N. D. Suryani, S. T. Rahayu, and U. Ardiningsih, "Optimalisasi teknologi biometrics dalam program e-KTP dengan penambahan data struktur gigi dan kartu sakti sebagai alternatif satu kartu multifungsi," *Jurnal Ilmiah Mahasiswa*, vol. 4, no.1, pp. 18-25, 2019.

[4] S. Hemalatha, "A systematic review on fingerprint-based biometric authentication system," In Proc. International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE), IEEE, 2020, pp. 1-4.

[5] Vandana and N. Kaur, "A Study of biometric identification and verification system," In Proc. International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE*)*, IEEE, 2021 pp. 60-64.

[6] K. Ab Wahab, L. W. Yew, and N. A. Jusoh, "Online attendance system using face recognition," *Engineering, Agriculture, Science and Technology Journal*, vol. 1, no. 1, pp. 57-61, 2022.

[7] M. Kushal, K. Kumar B.V., C. Kumar M.J., and M. Pappa, "ID

Card detection with facial recognition using Tensorflow and OpenCV," In Proc. 2nd International Conference on Inventive Research in Computing Applications, IEEE, 2020, pp. 742-746.

[8] T. Pinthong, W. Yimyam, N. Chumuang, and M. Ketcham, "Face recognition system for financial identity theft protection," In Proc. 15th International Joint Symposium on Artificial Intelligence and Natural Language Processing (iSAI-NLP), IEEE, 2020, pp. 1-6.

[9] S. Singh, and S. G. Jasmine. "Face recognition system," *International Journal of Engineering Research & Technology*, vol. 8, no. 05, pp. 263-266, 2019.

[10] A. Beno Lukito and R. Munadi, "Implementasi pengenalan wajah untuk keamanan rumah berbasis IoT menggunakan Raspberry Pi," *e-Proceeding of Engineering*, vol.8, no.4, pp. 3857-3866, 2021.

[11] R. V. Virgil Petrescu, "Face recognition as a biometric application," *Journal of Mechatronics and Robotics*, vol. 3, no. 1, pp. 237-257, 2019.

[12] A. Alzu'bi, F. Albalas, T. Al-Hadhrami, L. B. Younis, and A. Bashayreh, "Masked face recognition using deep learning: A review," *Electronics (Switzerland)*, vol. 10, no. 21, pp. 1-35, 2021.

[13] M. Taskiran, N. Kahraman, and C. E. Erdem, "Face recognition: Past, present and future (a review)," *Digital Signal Processing*: *A Review Journal*, vol. 106. Elsevier Inc., pp.1-28, 2020.

[14] J. I. V Luna, G. S Guzmán, J. F. C Aceves, F. J. S. Rangel, V. N. T Vargas, and M. A. L Acosta, "Access system using facial recognition and NFC," *International Research Journal of Advanced Engineering and Science*, vol. 8, no. 1, pp. 193-198, 2023.

[15] M. Fansyuri and D. Yunita, "Implementasi K-nearest neighbor untuk klasifikasi jenis kelamin berdasarkan analisis citra wajah," *Media Online*, vol. 3, no. 6, pp. 1208-1216, 2023.

[16] X. Guo, "A KNN classifier for face recognition," In Proc. 3rd International Conference on Communications, Information System and Computer Engineering (CISCE), IEEE, 2021, pp. 292-297.

[17] R. Mamoun, M. Nasor, and S. H. Abulikailik, "Design and development of mobile healthcare application prototype using Flutter," In Proc. International Conference on Computer, Control, Electrical, and Electronics Engineering (ICCCEEE), IEEE, 2021, pp. 1-6.

[18] S. Boukhary and E. Colmenares, "A clean approach to flutter development through the Flutter clean architecture package," In Proc. 6th Annual Conference on Computational Science and Computational Intelligence (CSCI), IEEE, 2019, pp. 1115-1120.

[19] S. Y. Ameen and D. Y. Mohammed, "Developing cross-platform library using Flutter," *European Journal of Engineering and Technology Research*, vol. 7, no. 2, pp. 18–21, 2022.

[20] M. Sävmarker, "How to design a digital guide app in Flutter/ Firebase with a focus on the group experience and text-to-speech," Thesis, Linköping University, 2023.

[21] H. D. R. Juliana, V. Naveen Kumar, G. Ricahard, and P. Shivadarshini, "Evecurate – A smart event management app using flutter and firebase," *International Journal of Scientific Research & Engineering Trends*, vol. 7, no. 4, pp. 2519-2524, 2020.

[22] I. F. Maulana, "Penerapan firebase realtime database pada aplikasi E-Tilang smartphone berbasis mobile android," *Jurnal Rekayasa Sistem dan Teknologi Informasi,* vol. 1, no. 3, pp. 854-863, 2019.

[23] S. Olenik, H. S. Lee, and F. Güder, "The future of near-field communication-based wireless sensing," *Nature*, vol. 6, no. 2021, pp. 286-288, 2021.

[24] S. S. Sengar, U. Hariharan, and K. Rajkumar, "Multimodal biometric authentication system using deep learning method," In Proc. International Conference on Emerging Smart Computing and Informatics (ESCI), IEEE, 2020, pp. 309-312.

[25] I. Markoulidakis, G. Kopsiaftis, I. Rallis, and I. Georgoulas, "Multi-class confusion matrix reduction method and its application on net promoter score classification problem," In Proc. International Conference Proceeding Series, ACM, 2021, pp. 412-419.