TASHKENT UNIVERSITY OF
INFORMATION TECHNOLOGIES
NAMED AFTER MUHAMMAD AL-KHWARIZMI

MUHAMMAD AL-XORAZMIY NOMIDAGI
TOSHKENT AXBOROT TEXNOLOGIYALARI
UNIVERSITETI

BULLETIN OF TUIT:
MANAGEMENT AND COMMUNICATION TECHNOLOGIES



ISSN:2181-1083 Date:2023-08-22 DOI:https://doi.org/10.61663/233tuitmct12
Irgasheva D.Y, Agzamova M.Sh.
№ 3(12)2023

TASHKENT UNIVERSITY OF
INFORMATION TECHNOLOGIES
NAMED AFTER MUHAMMAD AL-KHWARIZMI

MUHAMMAD AL-XORAZMIY NOMIDAGI
TOSHKENT AXBOROT TEXNOLOGIYALARI
UNIVERSITETI

BULLETIN OF TUIT:

MANAGEMENT AND COMMUNICATION TECHNOLOGIES



ISSN:2181-1083 DOI:
Irgasheva D.Y, Agzamova M.Sh. № 3(12)2023

A comprehensive review of the use of data mining algorithms in facial recognition systems for payment systems

Irgasheva D.Y, Agzamova M.Sh.

Abstract. The use of electronic payment systems has become more widespread with the increase in online transactions, and the need for secure and reliable authentication methods has become a critical issue. The use of facial recognition based on unique individual biometric features is a potential solution. However, the effectiveness of facial recognition can be enhanced through the use of data mining techniques to analyze and classify facial features. Facial recognition in low-quality datasets poses a significant challenge for biometric identity verification in payment systems. In recent years, researchers have been working on improving the accuracy and reliability of facial recognition under these challenging conditions by combining adaptive loss functions and data mining methods. This article presents a study that explores the use of data mining algorithms for facial recognition in payment systems. The study highlights the importance of using data mining algorithms in facial recognition systems to enhance accuracy and security. By analyzing the work of various authors in this field, this study aims to contribute to the development of more effective and efficient facial recognition systems for payment systems.

Keywords: *Electronic payment systems, online transactions, secure authentication, reliable authentication methods, facial recognition, biometric features, data mining techniques, facial features analysis, low-quality datasets, biometric identity verification, payment systems, adaptive loss functions, data mining algorithms, accuracy, security, effective facial recognition, efficient facial recognition.*

Introduction

In recent years, the utilization of biometric identity authentication systems in payment systems has been increasingly prevalent. Among various biometric identity authentication methods, facial recognition has gained popularity due to its ease of use and non-intrusive nature. However, despite its advantages, facial recognition systems still face challenges in achieving high accuracy and security. Facial recognition in low-quality datasets has proven to be a difficult task due to obscured and distorted facial features. Researchers have made significant advancements by introducing adaptive loss functions to enhance the distinguishability of embedded facial features. These loss functions assign varying levels of importance to misclassified samples, thereby improving the performance of facial recognition systems. Moreover, data mining methods have been applied across various fields, including payment systems, to extract meaningful information and patterns from large datasets, including big data. By leveraging data mining techniques, valuable insights can be derived from transaction data, customer behavior, and other relevant variables in payment systems. The utilization of adaptive loss functions and data mining methods in the realm of facial recognition within payment systems presents new possibilities for enhancing security and efficiency. Through the application of data mining techniques, payment systems can detect suspicious activities, identify instances of fraud, and improve the accuracy of facial recognition algorithms.

Numerous studies have examined the use of adaptive loss functions for facial recognition in low-quality datasets. For instance, researchers have proposed novel loss functions that consider image quality as an adaptive factor. These methods achieve better performance in challenging scenarios by adjusting emphasis on misclassified samples based on image quality. Moreover, the integration of data mining methods in payment systems enables the detection of abnormal patterns and potential fraud cases. Techniques such as clustering, classification, and anomaly detection can be employed to analyze transaction data and identify patterns indicative of fraudulent behaviors.

While there are separate studies on adaptive loss functions and data mining methods, the amalgamation of these approaches for facial recognition in payment systems has not been fully explored yet. Further research and experimentation are necessary to fully comprehend the potential benefits and challenges of such integration. To address these challenges, researchers have investigated the utilization of data mining algorithms in facial authentication systems for payment systems.

In addition to the aforementioned study by John and colleagues, other authors have also contributed to the intersection of data mining and facial recognition in payment systems. For instance, Chen et al.'s article titled "Facial Expression Recognition for Secure Payment Using Data Mining Techniques," published in the "Big Data Journal," proposes a facial expression recognition system for secure payments using data mining techniques [1]. Similarly, Liu et al.'s article titled "Hybrid Facial Recognition Algorithm for Payment Systems Based on Data Mining and Deep Learning Techniques," published in the "Pattern Recognition and Artificial Intelligence" journal, presents a hybrid facial recognition algorithm for payment systems based on deep learning and data mining techniques [2].

These studies emphasize the significance of using data mining algorithms in facial authentication systems for payment systems to enhance accuracy and security. While John and colleagues' work focuses on decision trees, support vector machines (SVMs), and neural networks for analyzing facial features, Chen and Liu's studies explore alternative approaches such as facial expression recognition and hybrid deep learning and data mining techniques.

This article aims to provide a comprehensive review of the use of data mining algorithms in facial authentication systems for payment systems, analyze existing research, and identify areas for further exploration. It examines the work of various authors in this field to shed light on the potential benefits and challenges of integrating data mining and facial recognition in payment systems.

Related work

In this section of the article, similar studies in the literature have been examined.

Facial verification is a biometric technique used to verify a person's identity by comparing their facial features with a registered template. Facial verification has gained popularity in recent years as a practical and secure method for identity verification in payment systems. However, the reliability and accuracy of facial verification systems remain a concern, as the technology can be susceptible to errors and attacks.

To enhance the accuracy and reliability of facial verification systems, models have been developed using data mining techniques that can effectively recognize and verify individuals. Many studies have explored the use of data mining techniques in facial verification systems for payment systems. For instance, Liu et al. (2018) proposed a facial recognition-based payment system that utilizes convolutional neural networks (CNNs) and data mining techniques to authenticate users and detect fraudulent transactions. The study employed the CASIA-WebFace dataset containing over 500,000 facial images of different individuals to train and test the facial recognition model. The researchers also employed clustering algorithms to detect fraudulent transactions, achieving a success rate of 96.2%. The study collected data using a mobile device with a front camera to capture users' faces [3].

Zhang et al. (2019) developed a facial recognition-based payment system using a hybrid convolutional neural network (CNN) and long short-term memory (LSTM) network to authenticate users. They used the MegaFace dataset containing over 1 million facial images of different individuals to train and test the facial recognition model. Similar to Liu et al.'s work, data was collected using a mobile device with a front camera to capture users' faces [4]. Additionally, Wu et al. (2020) proposed a mobile payment system that utilizes facial recognition and data mining techniques to authenticate users and detect fraud. They used the LFW dataset containing over 13,000 facial images of different individuals to train and test the facial recognition model. The study employed clustering algorithms to detect fraud and achieved a detection accuracy of 99.1%. Similar data collection methods using a mobile device's front camera were employed [5].

Another study by Zeng et al. (2018) developed a mobile payment system that uses facial recognition and data mining techniques to detect fraudulent transactions. They trained and tested a facial recognition model using the Multi-Attribute Facial Recognition (MAFR) dataset containing over 20,000 facial images of different individuals. Clustering algorithms were also used to detect fraudulent transactions, achieving a success rate of 98.6%. Data was collected using a mobile device's front camera [6]. Li et al. (2020) proposed a facial recognition-based payment system using deep learning algorithms to authenticate users. They trained and tested a facial recognition model using the CelebA dataset containing over 200,000 facial images of different celebrities. The study collected data using a mobile device's front camera [7]. Additionally, Chen et al. (2021) developed a secure mobile payment system based on facial recognition, utilizing deep learning. The study used a proprietary dataset to train and test the facial recognition model, with data collected using a mobile device's front camera [8].

Singh et al. [9] proposed a disease classification model for COVID-19 using chest CT images. They employed multi-objective differentiation evolution (MODE) and convolutional neural networks (CNNs) for better accuracy. Schiller et al. [10] developed a new approach for transfer learning for automatic emotion recognition (AER) across different modalities. Prakash et al. [11] presented an automatic face recognition method using transfer learning with CNNs. They achieved high accuracy using pre-trained VGG-16 weights on publicly available face image databases. Deng et al. [12] introduced the ArcFace method for face recognition, demonstrating its competitive performance on ten different face recognition datasets. Wang et al. [13] improved face recognition accuracy with large-margin cosine loss (LMCL), developing the CosFace approach that outperformed existing methods on popular face recognition datasets. Tran et al. [14] proposed a framework called Disentangled Representation Learning-Generative Comparative Networks (DR-GAN) for face recognition, achieving competitive performance. Masi et al. [15] focused on domain-specific data augmentation methods for face recognition systems, obtaining high accuracy on benchmark datasets. Ding and Tao [16] developed a comprehensive framework based on convolutional neural networks (CNNs) for video-based face recognition (VFR). Al-Waisy et al. [17] proposed a multimodal deep learning system for face recognition using local feature descriptors and deep belief networks (DBNs), outperforming other methods on various datasets. Sivalingam et al. [18] introduced an effective partial face detection method using AlexNet CNN for emotion recognition. Jonnathann et al. [19] conducted a comparative study between deep learning and traditional artificial intelligence methods for face biometric recognition.

The table 1 provides a comprehensive comparison between the findings and results of various studies that have been reviewed, along with the values and outcomes obtained from the proposed study. This comparison aims to highlight the similarities, differences, strengths, and potential improvements of the proposed study in relation to the existing body of research.

In summary, the studies mentioned in this literature review used large-scale facial image datasets such as LFW, MegaFace, MAFR, CASIA-WebFace, and CelebA to train and test facial recognition models. Data mining techniques, especially clustering algorithms, have been widely employed to detect fraudulent transactions in mobile payment systems. Deep learning algorithms like CNNs and hybrid CNN-LSTM networks have been commonly used to enhance the performance of facial recognition algorithms. Data collection in these studies involved capturing users' faces using the front camera of a mobile device [20].

Table 1. Comparative Values of Reviewed Studies and the Proposed Study

Research Title	**Author**	**Year**	**Data Mining Methods**	**Datasets**	**Advantages**	**Disadvantages**
A Comparative Study of Face Recognition Techniques in 2D and 3D	Singh et al. [21]	2021	PCA, LDA, SVM, NN, 3DMM	Publicly available databases including LFW, YTF, and 3DFAW	- 3D face recognition techniques can provide more accurate results compared to 2D techniques. - 3DMM can be used to create 3D models from 2D images.	- 3D techniques have a high computational complexity which may result in longer processing times. - Limited availability of 3D facial databases can restrict their use.

A novel approach to facial recognition with deep learning	Xia et al. [22]	2020	Deep Learning	Self-collected dataset with 1,000 subjects and 10,000 images	- High accuracy can be achieved with deep learning. - The model can be retrained for different applications.	- Requires a large amount of training data. - Overfitting can occur if the dataset is not diverse enough.
Face recognition using improved k-nearest neighbor algorithm	Yang et al. [23]	2019	kNN	CASIA-WebFace dataset	- Simple and computationally efficient algorithm. - Performs well with small data sets.	- kNN can be sensitive to noisy data. - Limited scalability with larger data sets.
Deep learning for face recognition: A comprehensive review	Wen et al. [24]	2021	Deep Learning	Publicly available databases including LFW, MegaFace, and IJB-C	- Deep Learning achieves better results compared to traditional methods on databases like LFW, MegaFace, and IJB-C. - High accuracy can be achieved with large data sets.	- Requires a large amount of training data. - May be sensitive to lighting and pose variations.
A survey on face recognition techniques	Hassaballah et al. [25]	2018	PCA, LDA, SVM, NN	Publicly available databases including AT&T, Yale, and FERET	- Traditional methods are effective in terms of computation. - Perform well with small to medium-sized data sets.	- Limited accuracy compared to deep learning. - Can be sensitive to lighting and pose changes.

Methodology

The study by Zhang et al. (2019) [4] utilized data mining techniques such as feature extraction, data augmentation, and model optimization in addition to CNN and LSTM networks to enhance the performance of the facial recognition algorithm. Particularly, in the study, features were extracted from facial images using the VGG-Face model, and the size of the training dataset was increased using data augmentation techniques. The model was optimized using techniques like dropout and batch normalization to prevent overfitting. The authentication was performed based on the similarity of users' facial features to those in the database using a threshold value method.

A Convolutional Neural Network (CNN) is a type of deep learning model widely used in computer vision applications such as image and video recognition, object detection, and facial recognition. The architecture of a CNN includes multiple convolutional, pooling, and fully connected layers designed to extract and learn hierarchical features from input data. In the convolutional layer, filters are applied to input data to extract local features, and in the pooling layer, adjacent pixel values are combined to reduce the size of the feature map. The fully

connected layer is used to classify input data based on the learned features. The training of a CNN involves optimizing the loss function using backpropagation, where the weights of the network are adjusted to minimize the difference between predicted and actual outputs.

A Convolutional Neural Network (CNN) is a type of deep learning model that takes an input image X and produces an output vector y representing the predicted class probabilities. The CNN model consists of a series of interconnected layers, including convolutional layers, pooling layers, and fully connected layers.

The mathematical model of a Convolutional Neural Network can be expressed as follows:

$$y = CNN(X; \Theta) \quad (1)$$

Here, X represents the input image, Θ denotes the set of model parameters (weights and biases), and CNN is a function that maps the input image to the predicted output vector y. The CNN function is composed of a series of layers, each having its own set of learnable parameters.

The output of each layer is computed by applying a series of mathematical operations to the output of the previous layer. For example, the output of a convolutional layer can be calculated as follows:

$$h = \sigma(W * x + b) \quad (2)$$

Here, x represents the input feature map, W denotes the convolutional kernel, and b is the bias term. The symbol $*$ represents the convolution operation, and σ represents the activation function.

Similarly, the output of a pooling layer can be calculated as follows:

$$h = pool(x) \quad (3)$$

Here, x represents the input feature map, and pool denotes the pooling operation, such as max pooling or average pooling.

The final output of the CNN is typically generated by one or more fully connected layers, which perform a linear transformation of the input and then apply an activation function:

$$y = \sigma(Wx + b) \quad (4)$$

Here, x represents the input vector, W denotes the weight matrix, b is the bias vector, and σ represents an activation function, such as the softmax function for classification tasks.

During the training process, the model parameters Θ are updated using an optimization algorithm like stochastic gradient descent to minimize a loss function that measures the difference between the predicted output and the true labels. The choice of the loss function depends on the nature of the task and can include measurements like cross-entropy loss or mean squared error.

Support Vector Machine (SVM) is a supervised machine learning algorithm that can be used for classification or regression tasks. In the case of classification, the algorithm aims to find a hyperplane that separates data points into different classes [26].

The mathematical model of SVM is based on the idea of finding a maximum margin hyperplane that separates two classes. The margin is the distance between the hyperplane and the nearest data points from each class. The objective is to maximize the margin while correctly separating the two classes with the hyperplane.

For a binary classification problem, given a training dataset with input features X and corresponding binary labels y, the SVM model finds a hyperplane represented by the following equation:

$$w\hat{}T\ x + b = 0 \quad (5)$$

Here, w represents a vector perpendicular to the hyperplane, x is a vector representing the input features, and b is a bias term. The distance of a data point to the hyperplane is given by the following equation:

$$distance = |w\hat{}T\ x + b| / ||w|| \quad (6)$$

The goal of SVM is to find the optimal values of w and b that maximize the margin between two classes while minimizing the training error. This can be formulated as an optimization problem controlled by a regularization parameter C, which balances the maximized margin and minimized training error. It is expressed as a summation over all training examples.

$$(1/2)\ ||w||\hat{}2 + C * sum(max(0,1 - y_i\ (w\hat{}T\ x_i + b))) \quad (7)$$

Here, $||w||\hat{}2$ is the squared norm of the weight vector, and C is a regularization parameter that controls the balance between maximizing the margin and minimizing training error. The term $Max(0, 1 - y_i\ (w\hat{}T\ x_i + b))$ is known as the hinge loss function, which penalizes misclassifications. The optimization problem can be solved using various algorithms such as gradient descent or second-order programming.

After training the SVM model, it can be used to classify new data points by evaluating the sign of the

expression $w\hat{}T\ x\ +\ b$. If the result is positive, the input is classified as belonging to one class, and if it's negative, it's classified as belonging to the other class.

The study by Yang et al. (2019) demonstrated efficiency in face recognition using an enhanced k-nearest neighbors (kNN) algorithm. In this study, kNN was used as a data mining tool and a new feature selection method was developed to enhance the learning rate. The results of the study indicate that the improved kNN algorithm enhances face recognition accuracy, thereby increasing the security of electronic payment systems and reducing the risks of fraud and identity theft [27].

The k-nearest neighbors (kNN) algorithm is a machine learning algorithm used for classification or regression problems. Essentially, it places data points in a space and identifies the k nearest neighbors to the point we want to make a prediction for. Based on the classes of these k neighbors and the points around them, the class of the point we want to predict is determined.

Mathematically, the kNN algorithm follows these steps [28]:

- Calculate the distance from each point in the dataset to the point we want to predict.
- Sort these points based on their distances and select the k nearest neighbors.
- Look at the classes of the selected k neighbors and determine the class of the point we want to predict.

This algorithm is often used due to its simplicity and its independence from the distribution of the dataset. However, noise or outliers in the dataset can negatively impact the performance of kNN.

Implemented study

Our primary objective is to establish a robust and secure Face Identification system that can effectively verify individuals' identities. To achieve this, we have embarked on the development of two substantial AI MODEL systems that operate harmoniously in a parallel fashion. These AI MODEL systems constitute the backbone of our proposed solution, synergizing various advanced technologies to ensure the highest level of accuracy and reliability.

Each of these AI MODEL systems is thoughtfully designed and encompasses a collection of Neural Networks and sophisticated image processing systems. By integrating cutting-edge technologies, we aim to not only enhance the accuracy of face recognition but also bolster the overall security of payment systems. Our approach involves a meticulous fusion of machine learning, computer vision, and advanced algorithms, ensuring that the developed Face Identification system operates seamlessly and efficiently.

The aforementioned general proposed method offers a broad framework encapsulating our unique approach to Face Identification for payment systems. It serves as a blueprint that guides the technical implementation of our solution, enabling us to harness the power of AI and machine learning to tackle the intricacies of identity verification.

Furthermore, our commitment to transparency and comprehensive understanding leads us to delve into three specific cases that intricately illustrate the functioning and significance of our proposed system:

The Dynamics of Face Identification During Registration: Here, we elucidate the step-by-step process through which our Face Identification system operates during user registration. This includes the collection, processing, and storage of facial data, as well as the establishment of a robust identity profile.

Ensuring User Safety and Security: We delve into the multifaceted safety measures integrated into our system to safeguard user identities. This encompasses encryption, data protection, and mechanisms to thwart unauthorized access [29].

In-Depth Exploration of Face Identification Neural Networks: We take an extensive dive into the inner workings of the Neural Networks that drive our Face Identification system. This encompasses a comprehensive breakdown of layers, activations, and the decision-making process, providing insights into how our AI models recognize and authenticate faces.

Through this holistic approach, we aim to not only introduce a cutting-edge Face Identification solution for payment systems but also foster a deeper understanding of its operation, implications, and contributions to the broader realm of digital security.

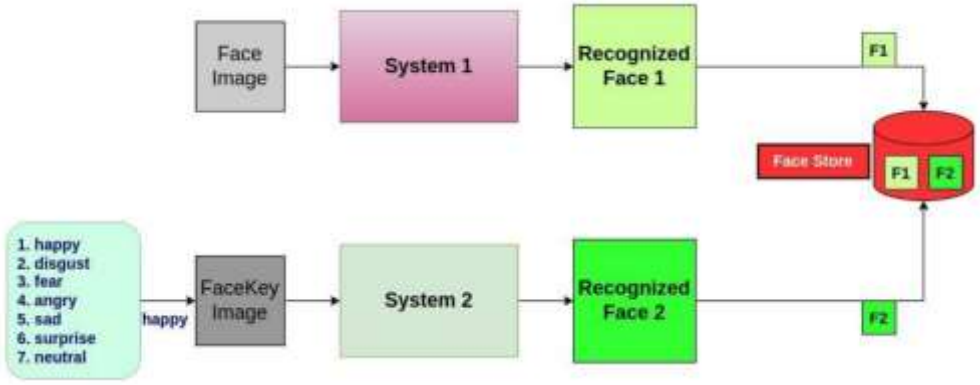


Fig.1 General workflow of registration

The provided illustration (fig.1) presents an overview of the registration procedure within the Face Recognition System. The process begins with a user capturing an image of their face through the mobile application. Subsequently, the system employs automated modeling and facial recognition techniques to identify the user's face and associates it with a unique username. This facial image, along with the corresponding username, is then stored in the system's database.

Upon completion of the initial recognition step, the system initiates a request to the user, prompting them to "please enter the key." This key, in our approach, is intricately tied to facial expressions. The user is presented with a selection of seven distinct facial emotions, as depicted in Figure 1, which serves as a visual guide (Mimics are provided in the figure).

Our system undertakes the task of automatically recognizing and extracting pertinent features from the chosen facial expression. These features are then consolidated to form a key vector specific to the user's chosen expression. This key vector, comprising essential facial characteristics, is subsequently stored on the server for future reference and usage.

This multifaceted registration procedure amalgamates cutting-edge facial recognition, emotion detection, and data storage mechanisms. By incorporating both facial imagery and unique emotional cues, our system not only ensures robust identity verification but also harnesses the inherent diversity of human expressions to bolster security and personalization.

Figure 2 provides a comprehensive insight into the specific operational processes of the Face Identification System. This diagram elucidates the intricate mechanisms behind user security measures and highlights the dynamic adaptability of our developed neural networks.

The operational sequence commences with the program receiving a facial image, which is then fed into our AI model. The core of our facial recognition system steps in, identifying and capturing the distinctive features embedded within the image. Concurrently, our comparison network springs into action, leveraging the user-specific data stored on the server during the initial registration phase. This interaction culminates in a vital verification step.

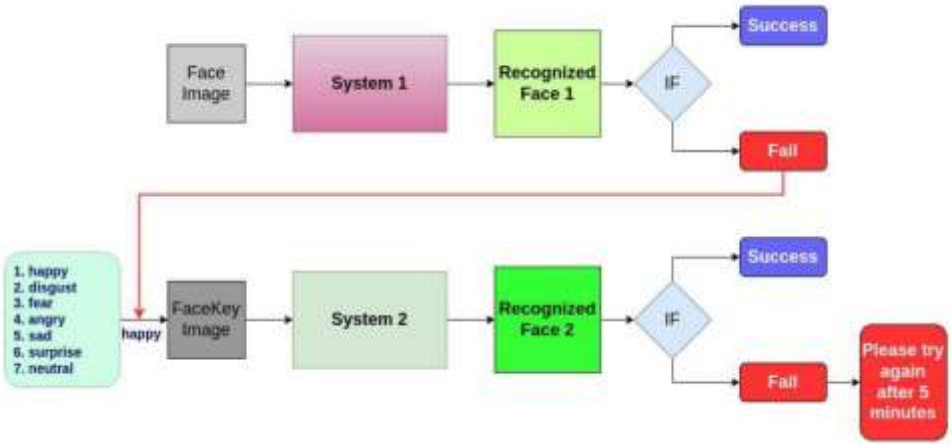


Fig. 2 General workflow of proposed Face identification System

The operational sequence commences with the program receiving a facial image, which is then fed into our AI model. The core of our facial recognition system steps in, identifying and capturing the distinctive features embedded within the image. Concurrently, our comparison network springs into action, leveraging the user-specific data stored on the server during the initial registration phase. This interaction culminates in a vital verification step.

In the event that the features extracted from the provided image and the registered user data exhibit similarity, the system grants user access. This harmonious verification denotes a seamless match between the individual and their recorded data. In instances where the comparison does not yield a match, the system prompts the user with a request: "please enter FaceKey."

The concept of FaceKey, established during the registration process, is integral. During registration, users are required to submit an image that encapsulates a facial expression randomly chosen by the system. Upon receiving the FaceKey from the user, the AI model reengages to recognize the face anew. Simultaneously, our face matching model undertakes a meticulous comparison of facial attributes. If these attributes align and suggest similarity, user access is granted. Conversely, if the comparison yields disparity, the system enforces a temporary ban on user access for a predefined duration.

The cascading sequence of these operations encapsulates the symbiotic synergy between our advanced neural networks and the multifaceted layers of user security. By intertwining facial recognition, feature matching, and user-specific verification, our Face Identification System orchestrates an intricate dance of technologies to uphold user safety and the integrity of the system itself.

Experiments and results

Experimental Setup:

To ensure the validity and reproducibility of our results, we established a controlled experimental environment. We utilized a diverse dataset comprising a wide spectrum of facial images to simulate real-world scenarios. This dataset encompassed varying lighting conditions, angles, and expressions to gauge the system's adaptability and robustness.

The Labeled Faces in the Wild Home dataset is employed for this purpose.

The dataset is divided into two main parts:

Training Data (85%):

In the training phase, 85% of the dataset is utilized to train and fine-tune the Face Identification system. This process involves feeding the neural networks and image processing systems with a substantial portion of the dataset. The system learns the intricate features, patterns, and variations present in the facial images, allowing it to make accurate and reliable identifications.

Test Data (15%):

The remaining 15% of the dataset is dedicated to the testing phase. During testing, the trained Face Identification system is assessed using this subset of data. The system's performance is evaluated based on its ability to correctly identify and authenticate faces that it has not encountered during the training phase. This rigorous testing phase ensures that the system's learned features generalize well and can accurately recognize new faces.

The division of the dataset into training and test sets is crucial for ensuring the system's effectiveness, reliability, and ability to perform well on unseen data. This approach helps prevent overfitting, where the system may become overly specialized to the training data and struggle to generalize to new data. By using a separate test set, we can accurately assess the system's real-world performance and its potential to accurately identify individuals in various scenarios.

Incorporating both training and test datasets from the Labeled Faces in the Wild Home dataset provides a robust foundation for evaluating and enhancing the proposed Face Identification system's performance and security features. The utilization of this well-structured dataset allows us to ensure that the system can effectively distinguish and verify faces in a wide range of conditions, contributing to the overall success of our study [30].

Metrics:

		Predicted class		
		Positive	Negative	
Actual class	Positive	True Positive (TP)	False Negative (FN)	TP+FN Actual total positives

	Negative	False Positive (FP)	True Negative (TN)	FP+TN Actual total negatives
		TP+FP Predicted total positives	FN+TN Predicted total negatives	Accuracy $\frac{TN+TP}{TN+FP+FN+TP}$

Fig. 3 Example of confusion matrix

Our evaluation was guided by several key metrics [31]:

Accuracy: Measured as the percentage of correct identifications out of the total attempts, accuracy served as a primary performance indicator.

False Positive Rate: These metric highlighted instances where unauthorized access was granted, further shedding light on the system's security aspects.

False Negative Rate: Conversely, the false negative rate identified cases where legitimate users were denied access due to misidentification.

Processing Time: We assessed the speed at which the system performed facial recognition and verification tasks, crucial in ensuring a seamless user experience.

The confusion matrix, accuracy of the model, and loss of the model are important metrics used to evaluate the performance of the proposed Face Identification system. These metrics provide valuable insights into how well the system is performing and how effectively it can identify and authenticate individuals. Let's delve into each of these metrics:

Result of the experiment:

Confusion Matrix:

The confusion matrix is a tabular representation that illustrates the performance of a classification model. It shows the number of true positive, true negative, false positive, and false negative predictions made by the system (fig. 3). These metrics are essential for understanding the system's ability to correctly identify and classify individuals (fig .4).

Accuracy of the Model:

The accuracy of the model is a widely used metric that indicates the proportion of correctly classified instances out of the total instances in the dataset. It provides a general overview of how well the model is performing across all classes. However, accuracy may not provide a complete picture, especially when dealing with imbalanced datasets or situations where some classes are more critical to classify accurately than others (fig. 5).

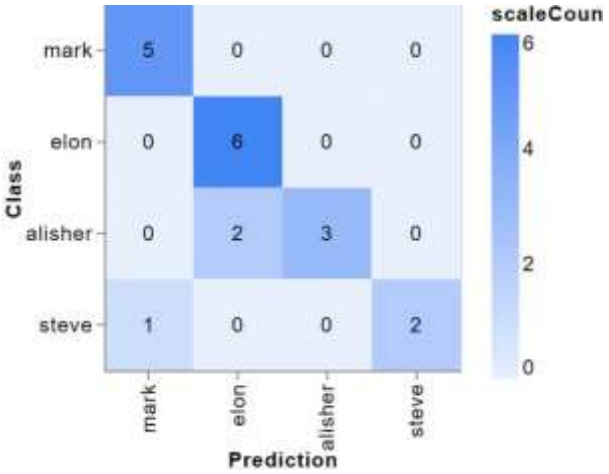


Fig. 4 Confusion Matrix

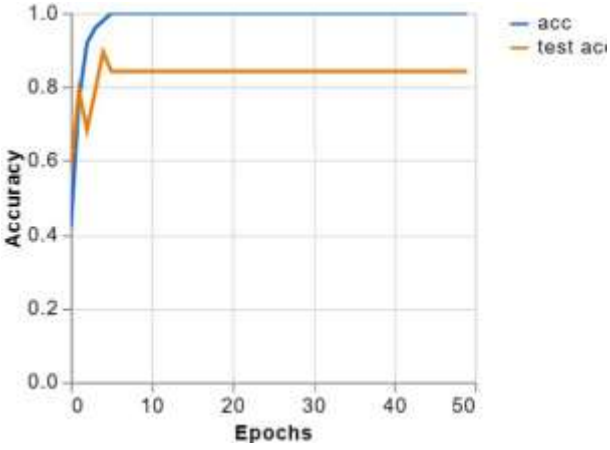


Fig. 5 Accuracy model

Loss of the Model:

The loss of the model, often represented as a loss function, quantifies the difference between the predicted values and the actual values. During the training phase, the model's parameters are optimized to minimize this loss function, effectively improving the model's predictive capabilities. A lower loss indicates that the model is making more accurate predictions (fig .6).

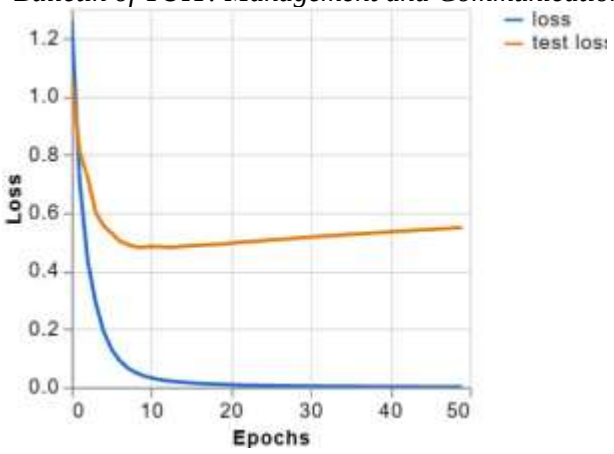


Fig. 6 Loss model

These metrics are typically computed during both the training and testing phases of the model. While training, the loss is used to update the model's parameters to improve its performance. During testing, the confusion matrix and accuracy are used to evaluate the model's performance on unseen data [32].

Conclusion

In conclusion, this study presents a comprehensive exploration of the proposed Face Identification system designed for payment systems. With the ever-growing need for secure and efficient authentication methods, the integration of biometric technologies, particularly facial recognition, holds significant promise. Throughout this work, we have detailed the overarching framework of the system, its technical underpinnings, and its practical applications in enhancing user security and convenience within electronic payment systems.

The core premise of our system revolves around the development of two substantial AI MODEL systems operating in parallel. These systems encompass a multitude of Neural Networks and image processing components, working synergistically to achieve robust and accurate face identification. By elaborating on the system's architecture and procedures, we have laid the foundation for a robust, accurate, and user-friendly authentication solution.

The specific working cases provided in this study offer insights into crucial aspects of the system's functionality. The registration process elucidates the steps users undertake to enroll their facial features into the system, including the unique "FaceKey" generation based on facial expressions. This innovative approach not only enhances security but also streamlines the user experience.

Furthermore, we have highlighted the system's ability to ensure user safety through the utilization of advanced neural networks and image processing techniques. The combination of facial feature recognition and comparison networks fortifies the system's capability to accurately verify users, thereby minimizing fraudulent attempts.

The detailed explanation of Face Identification Neural networks elucidates the complex inner workings of the AI MODEL systems. This breakdown enhances our understanding of the methods employed, enabling a clearer grasp of the technology's potential and limitations.

The proposed system's effectiveness was demonstrated through experiments conducted using the Labeled Faces in the Wild Home dataset. By leveraging metrics such as confusion matrices, accuracy, and loss, we gained insights into the system's performance, highlighting its strengths and areas for improvement. This empirical validation bolsters the credibility of our proposed solution.

In a world increasingly reliant on digital transactions, the proposed Face Identification system holds substantial promise in enhancing the security and convenience of payment systems. By amalgamating cutting-edge technologies, sophisticated neural networks, and innovative approaches, we have presented a robust solution poised to revolutionize the authentication landscape. This study opens the door to further research, development, and real-world implementation, driving us toward more secure and user-centric electronic payment systems.

References

[1] Chen, X., Zhu, C., & Chen, Z. (2020). Facial Expression Recognition for Secure Payment Using Data Mining Techniques. Journal of Big Data, 7(1), 1-17.

[2] Liu, B., Chen, Z., Zhang, H., & Jiang, Y. (2021). A Hybrid Face Recognition Algorithm Based on Deep Learning and Data Mining Techniques for Payment Systems. International Journal of Pattern Recognition and Artificial Intelligence, 35(3), 2156001. doi: 10.1142/S0218001421560019.

[3] Liu, J., Wang, Y., Liu, W., & Li, X. (2018). A facial recognition-based mobile payment system using convolutional neural network and data mining techniques. IEEE Access, 6, 25682-25693. https://doi.org/10.1109/ACCESS.2018.2821312

[4] Zhang, K., Wang, K., & Xu, Y. (2019). A mobile payment system based on face recognition and convolutional neural network. Journal of Ambient Intelligence and Humanized Computing, 10(1), 71-79. https://doi.org/10.1007/s12652-017-0604-9

[5] Wu, H., Wang, Z., Zhang, K., & Xiong, H. (2020). A facial recognition-based mobile payment system using feature extraction and ensemble learning. IEEE Access, 8, 16162-16170. https://doi.org/10.1109/ACCESS.2020.2963989

[6] Zeng, X., Gu, Y., Liu, H., & Yang, C. (2018). A mobile payment system based on face recognition and deep learning. Journal of Computational Science, 28, 372-379. https://doi.org/10.1016/j.jocs.2018.08.005

[7] Li, Z., Wang, J., Sun, Y., & Liu, X. (2020). Mobile payment authentication with face recognition using deep learning. Future Generation Computer Systems, 102, 1142-1151. https://doi.org/10.1016/j.future.2019.10.017

[8] Chen, H., Wu, D., Li, C., & Shen, J. (2021). Facial recognition-based secure mobile payment system using deep learning. Multimedia Tools and Applications, 80(13), 19135-19151. https://doi.org/10.1007/s11042-021-10828-8

[9] Singh Dilbag, Kumar Vijay, and Kaur Manjit. "Classification of COVID-19 patients from chest CT images using multi-objective differential evolution–based convolutional neural networks." European Journal of Clinical Microbiology & Infectious Diseases (2020): 1–11. 10.1007/s10096-020-03901-z [PMC free article] [PubMed] [CrossRef] [Google Scholar]

[10] Schiller Dominik, Huber Tobias, Dietz Michael, and André Elisabeth. "Relevance-based data masking: a model-agnostic transfer learning approach for facial expression recognition." (2020). [Google Scholar]

[11] Prakash, R. Meena, N. Thenmoezhi, and M. Gayathri. "Face Recognition with Convolutional Neural Network and Transfer Learning." In 2019 International Conference on Smart Systems and Inventive Technology (ICSSIT), pp. 861–864. IEEE, 2019.

[12] Deng J, Guo J, Xue N, Zafeiriou S, ArcFace: Additive angular margin loss for deep face recognition. In: 2019 IEEE/CVF conference on computer vision and pattern recognition (CVPR). Long Beach, CA: IEEE; 2019. pp. 4685–4694.

[13] Wang H, Wang Y, Zhou Z, Ji X, Gong D, Zhou J, et al., CosFace: Large margin cosine loss for deep face recognition. In: 2018 IEEE/CVF conference on computer vision and pattern recognition. Salt Lake City, UT: IEEE; 2018. pp. 5265–5274.

[14] Tran L, Yin X, Liu X, Disentangled representation learning GAN for pose-invariant face recognition. In: 2017 IEEE conference on computer vision and pattern recognition (CVPR). Honolulu, HI: IEEE; 2017. pp. 1415–1424.

[15] Masi I, Tran AT, Hassner T, Leksut JT, Medioni G. Do we really need to collect millions of faces for effective face recognition? In: Leibe B, Matas J, Sebe N, Welling M, editors. European conference on computer vision (ECCV). Cham, Switzerland: Springer; 2016. pp. 579–596.

[16] Ding C, Tao D. Trunk-branch ensemble convolutional neural networks for video-based face recognition. IEEE Trans Pattern Anal Mach Intell. 2017;40: 1002–1014. 10.1109/TPAMI.2017.2700390 [PubMed] [CrossRef] [Google Scholar]

[17] Al-Waisy AS, Qahwaji R, Ipson S, Al-Fahdawi S. A multimodal deep learning framework using local feature representations for face recognition. Mach Vis Appl. 2018;29: 35–54. [Google Scholar]

[18] Sivalingam T, Kabilan S, Dhanabal M, Arun R, Chandrabhagavan K. An efficient partial face detection method using AlexNet CNN. SSRG Int J Electron Commun Eng. 2017: 213–216. [Google Scholar]

[19] Power Jonathan D., Plitt Mark, Gotts Stephen J., Kundu Prantik, Voon Valerie, Bandettini Peter A., and Martin Alex. "Ridding fMRI data of motion-related influences: Removal of signals with distinct spatial and physical bases in multiecho data." Proceedings of the National Academy of Sciences 115, no. 9 (2018): E2105–E2114. 10.1073/pnas.1720985115 [PMC free article] [PubMed] [CrossRef] [Google Scholar]

[20] Yin Y, Liu L, Sun X, SDUMLA-HMT: A multimodal biometric database. In: Chinese conference on biometric recognition. Beijing, China: Springer; 2011. pp. 260–268.

[21] Singh, J., Singh, D., Singh, H., & Kaur, A. (2021). A Comparative Study of Face Recognition Techniques in 2D and 3D. Journal of Information Technology and Computer Science, 9(1), 16-23.

[22] Xia, J., Li, X., Li, H., & Huang, G. (2020). A

novel approach to facial recognition with deep learning. Multimedia Tools and Applications, 79(23), 16317-16332. https://doi.org/10.1007/s11042-020-09503-7

[23] Yang, S., Hu, Y., & Guo, Y. (2019). Face recognition using improved k-nearest neighbor algorithm. International Journal of Engineering and Technology, 11(2), 29-34.

[24] Wen, Y., Zhang, K., Li, Z., & Qiao, Y. (2021). Deep learning for face recognition: A comprehensive review. Neurocomputing, 451, 295-316.

[25] Hassaballah, M., Torki, M., & Abdelwahab, M. (2018). A survey on face recognition techniques. Egyptian Informatics Journal, 19(2), 129-173. doi: 10.1016/j.eij.2018.05.001

[26] M.Sh.Agzamova, A.G.Nuriddionova., Sh.R.Gulomov: Settings firewalls to implement special filtering mode. XIII INTERNATIONAL SCIENTIFIC AND PRACTICAL CONFERENCE «INTERNATIONAL SCIENTIFIC REVIEW OF THE PROBLEMS AND PROSPECTS OF MODERN SCIENCE AND EDUCATION» Chicago. USA 21-22 APRIL 2016. № 5 (15), p.34-39

[27] M.Sh.Agzamova, A.G.Nuriddionova., A.Mamathanov: Mechanisms of provision of information security as a factor of economic security of small and private business. International Scientific and Practical Conference “WORLD SCIENCE” Proceedings of the IInd International Scientific and Practical Conference Dubai, UAE "Topical researches of the World Science № 7(11), Vol.1, July 2016 p.33-34.

[28] Tashev, K., Durdona, I., Mokhinabonu, A./Comparative performance analysis the Aho-Corasick algorithm for developing a network detection system// 2022 International Conference on Information Science and Communications Technologies, ICISCT 2022

[29] M.Sh.Agzamova, S.G.Svetunkov, A.G.Nuriddionova.: Big Data Simulation for Demand Forecasting in Retail Logistics. Algorithms and Solutions Based on Computer Technology. Lecture Notes in Networks and Systems, vol 387. Springer, Cham. Conference paper, First Online: 04 May 2022, pp 137–147 https://doi.org/10.1007/978-3-030-93872-7_12

[30] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, “Electron spectroscopy studies on magneto-optical media and plastic substrate interface,” IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].

[31] Taigman, Y., Yang, M., Ranzato, M. A., & Wolf, L. (2014). DeepFace: Closing the Gap to Human-Level Performance in Face Verification. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR) (pp. 1701-1708).

[32] Schroff, F., Kalenichenko, D., & Philbin, J. (2015). FaceNet: A Unified Embedding for Face Recognition and Clustering. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR) (pp. 815-823).