**Deep Learning Based Multimodal Fusion: IRIS & Fingerprint**

**A Project Report**

***submitted by***

**Rajnish Kumar CS21B2031**

in partial fulfillment of requirements

for the award of the degree of

**BACHELOR OF TECHNOLOGY**

Department of **Computer Science and Engineering**

**INDIAN INSTITUTE OF INFORMATION TECHNOLOGY, DESIGN AND MANUFACTURING KANCHEEPURAM**

**2024**

ACKNOWLEDGEMENTS

I would like to express my sincere gratitude to all the individuals who have helped me throughout this project. First and foremost, I would like to thank my project supervisor and our Professor, Dr. Rahul Raman, for his guidance and support. His expertise, encouragement, and feedback were invaluable to the success of this project.

I also extend my thanks to the staff at IIITDM Kancheepuram, who provided us with the necessary resources and facilities to carry out this research.

Lastly, I would like to express my gratitude to my families and friends for their unwavering support and encouragement. Their patience and understanding helped me to stay focused and achieve my goals.

Thank you all for your support and guidance throughout this project.

ABSTRACT

This project focuses on the development of a multimodal biometric authentication system utilizing iris and fingerprint images. The goal is to leverage the complementary nature of these biometric modalities to enhance the accuracy and robustness of authentication systems. The proposed approach involves the extraction of discriminative features from iris and fingerprint images using local binary pattern (LBP) and gray-level co-occurrence matrix (GLCM) methods, respectively. These features are then fused at the feature level using a Siamese neural network architecture.

A Siamese neural network architecture is proposed to fuse the extracted features from iris and fingerprint modalities. The network consists of shared dense layers that learn joint representations from both modalities and a final classification layer for authentication.

The proposed system aims to achieve robust and reliable biometric authentication, suitable for various security applications such as access control, identity verification, and forensic analysis. The experimental results demonstrate the effectiveness of the multimodal fusion approach in improving authentication performance compared to single-modality systems.

TABLE OF CONTENTS

1. MULTI-MODAL BIOMETRICS

1.1 Motivation and Background

1.2 Multimodal Biometrics: A Promising Path

1.3 Research Objectives

1.4 Approach

1.5 Methodology

1.5.1 About Dataset

1.5.2 Tools Used

1.5.3 Creation of Database

1.5.4 Testing

1.6 Algorithms Used

1.6.1 Siamese Network

1.7 Code and Dataset

1.8 Results

1.9 Future Advancements

1.10 Flaws in the System

1.11 Conclusion

CHAPTER 1: MULTI-MODAL BIOMETRICS

**1.1 Motivation and Background**

Multimodal biometrics, which involve combining multiple biometric modalities such as fingerprints, iris scans, facial recognition, voice recognition, etc., have gained significant attention and traction due to their ability to address the inherent limitations and challenges faced by single-modal biometric systems. The motivation behind the development and adoption of multimodal biometrics stems from several key factors:

1. Limitations of Single-Modal Systems:

* Single-modal biometric systems, which rely on a single biometric trait for authentication, may encounter challenges in accuracy, especially in scenarios where environmental conditions or inherent variability in biometric traits impact performance. For example, fingerprint recognition systems may struggle with accuracy in cases of worn or damaged fingerprints, while facial recognition systems may face difficulties in low-light conditions or when facial features are obscured.

2. Vulnerability to Spoofing:

* Single-modal biometric systems are also susceptible to spoofing attacks, where imposters can present fake biometric traits to gain unauthorized access. For instance, fingerprint recognition systems can be fooled by spoof fingerprints created using materials like silicone or gelatin, while facial recognition systems may be deceived by presenting a photograph or a mask resembling the authorized user's face.

3. Robustness Concerns:

* Biometric traits can be influenced by various factors such as injury, illness, or aging, which may lead to changes in the biometric data over time. This variability can pose challenges in maintaining consistent performance and accuracy of single-modal biometric systems, particularly in long-term deployment scenarios.

The motivation for adopting multimodal biometrics lies in its potential to overcome these limitations and address the increasing demand for secure, robust, and user-friendly authentication solutions across diverse applications. By combining multiple biometric modalities, multimodal systems offer several advantages:

* Enhanced Accuracy:

By leveraging complementary information from multiple biometric traits, multimodal systems can achieve higher accuracy compared to single-modal systems. For example, combining fingerprint and iris recognition can provide a more reliable authentication mechanism by utilizing both physiological and behavioral biometric characteristics.

* Improved Security:

Multimodal biometric systems offer increased resistance to spoofing attacks by requiring multiple independent biometric traits for authentication. This multi-factor approach enhances security and makes it more difficult for imposters to bypass the authentication process.

* Increased Robustness:

By diversifying the sources of biometric data, multimodal systems can mitigate the impact of individual variability or environmental factors on authentication performance. This enhances the system's robustness and reliability over time, even in dynamic operating conditions.

* User-Friendly Authentication:

Multimodal biometric systems can provide a seamless and user-friendly authentication experience by offering multiple authentication options to users. This flexibility allows individuals to choose the most convenient and accessible biometric modality for authentication, enhancing user acceptance and adoption.

Overall, the motivation and background of multimodal biometrics underscore its potential to address the challenges faced by single-modal systems while meeting the evolving needs for secure and convenient authentication solutions in various domains such as security, access control, and identity management.

**1.2 Multimodal Biometrics: A Promising Path**

Multimodal biometrics represent a paradigm shift in biometric authentication systems, harnessing the power of multiple biometric modalities to overcome the inherent limitations of single-modal systems. The fusion of different biometric modalities such as iris scans and fingerprint scans offers a promising solution to enhance the security and accuracy of user authentication processes.

1. Integration of Strengths:

* Each biometric modality has its strengths and weaknesses. For example, iris recognition is known for its high accuracy and resistance to spoofing attacks, while fingerprint recognition offers high user acceptance and is widely deployed. By integrating these modalities, a multimodal system can leverage the strengths of each modality to compensate for the weaknesses of the others. For instance, combining iris and fingerprint scans can provide a more robust authentication mechanism that is both highly accurate and resistant to spoofing attempts.

2. Overcoming Limitations:

* Single-modal biometric systems may face challenges such as susceptibility to spoofing attacks, variability in biometric traits due to environmental factors, and limitations in accuracy under certain conditions. By integrating multiple modalities, multimodal systems can mitigate these limitations. For instance, while an iris scan may fail due to poor lighting conditions, a fingerprint scan can provide additional authentication data, enhancing the overall reliability of the system.

3. Research Focus on Iris and Fingerprint Fusion:

* The specific focus of this research project on the fusion of iris and fingerprint scans underscores the importance of leveraging two highly reliable and widely used biometric modalities. Iris recognition is characterized by its uniqueness and stability over time, while fingerprint recognition offers a convenient and widely accepted means of authentication. By combining these modalities, the research project aims to develop a robust and accurate multimodal biometric system that can be deployed in various real-world applications.

4. Enhanced Security and Accuracy:

* The ultimate goal of integrating iris and fingerprint scans is to enhance the security and accuracy of user authentication processes. Multimodal biometric systems offer increased resilience to spoofing attacks, improved accuracy in authentication, and greater reliability in diverse operating conditions. This heightened level of security and accuracy is crucial for applications such as access control, identity verification, and financial transactions, where the integrity of authentication systems is paramount.

**1.3 Research Objectives**

This research project aims to:

Develop a Multi-Modal Biometric system that utilizes iris recognition and fingerprint recognition for user authentication.

Evaluate the effectiveness of the proposed system in terms of recognition accuracy, security robustness, and computational efficiency.

Analyze the advantages and limitations of the Multi-Modal approach compared to traditional Uni-Modal systems.

- Identify potential future directions for improvement and advancement of the proposed system.

\*\*1.4 Approach\*\*

Our proposed Multi-Modal Biometric system tackles user authentication through a sequential pipeline. The system first captures iris and fingerprint images from the dataset. These images are then preprocessed and features are extracted using local binary pattern (LBP) for iris and gray-level co-occurrence matrix (GLCM) for fingerprint. The extracted features are then fused using a Siamese neural network architecture for authentication.

**1.5 Methodology:**

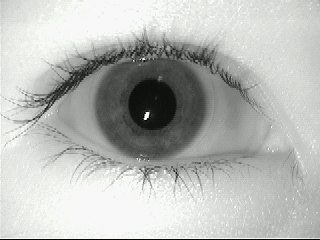
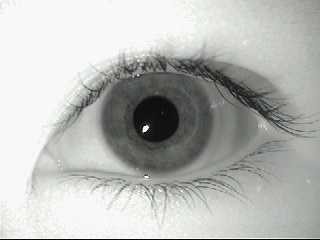
**1.5.1 About Dataset:**

The dataset used in this project consists of 45 subject. Dataset contains 5 scanned image of left and right iris and each finger’s print of the subject.





Above are the scanned images of left(above 5) & right (below 5) finger print.



Above are the left & right iris scan of the subject.

**1.5.2 Tools Used:**

The following tools and libraries were utilized in this project:

- Open CV for image processing

- NumPy for numerical computations

- TensorFlow for building and training neural networks.

- scikit-image for feature extraction

**1.5.3 Creation of Database:**

The creation of a database for iris and fingerprint features extraction using LBP (Local Binary Patterns) and GLCM (Gray-Level Co-occurrence Matrix) respectively is a pivotal step in establishing a robust recognition system for biometric identification. Feature extraction, a fundamental aspect of pattern recognition and computer vision, transforms raw image data into a format suitable for analysis by capturing distinctive characteristics inherent in the data. LBP, renowned for its efficacy in texture analysis, encodes local texture patterns by comparing pixel values with their neighbors, thus offering a nuanced representation of iris texture crucial for recognition tasks. On the other hand, GLCM, a statistical technique, provides insights into the spatial relationships between pixel pairs in an image, thereby revealing intricate patterns and ridges intrinsic to fingerprints.

In structuring the database, a relational approach is adopted, comprising two distinct tables: the Iris Features Table and the Fingerprint Features Table. The former stores iris features extracted through LBP, where each row corresponds to an iris sample and each column encapsulates a feature extracted from that sample. These features may include LBP histograms or other statistical descriptors. Conversely, the Fingerprint Features Table houses fingerprint features extracted using GLCM, following a similar row-column structure to encapsulate GLCM-derived metrics like contrast, correlation, energy, and entropy. This segregation optimizes storage efficiency and facilitates streamlined retrieval of specific feature sets, consequently enhancing the agility and effectiveness of recognition tasks.

By employing this database architecture, the system lays a robust foundation for future recognition endeavors. It not only ensures efficient storage and retrieval but also sets the stage for the development of advanced recognition algorithms capable of accurately identifying individuals based on their unique iris and fingerprint biometric traits.

**1.5.4 Testing:**

During the testing phase, iris and fingerprint images are captured, preprocessed to enhance quality, and subjected to feature extraction techniques like LBP for iris images and GLCM for fingerprints. These extracted features are then used for authentication via a Siamese neural network, which compares feature representations to determine individual identity. Performance evaluation focuses on accuracy, measuring the system's ability to correctly identify individuals, and computational efficiency, assessing processing speed and resource utilization. By analyzing these metrics, stakeholders can determine the effectiveness and suitability of the biometric recognition system for real-world deployment, guiding potential improvements to enhance accuracy and optimize computational performance.

**1.6 Algorithms Used**

**1.6.1 Siamese Network:**

The Siamese neural network architecture, integral to the biometric recognition system, operates by fusing features extracted from iris and fingerprint modalities through shared dense layers, enabling the learning of joint representations. These shared layers facilitate the extraction of essential information from both modalities simultaneously, allowing the network to establish meaningful correlations between iris and fingerprint features. Following this joint representation learning, a final classification layer is employed for authentication, utilizing the learned representations to distinguish between genuine and impostor pairs. During the authentication process, pairs of extracted features are passed through the network, which outputs a similarity score or probability indicating the likelihood of the pairs belonging to the same individual. Renowned for its capability to effectively fuse information from multiple modalities and handle complex similarity metrics, the Siamese neural network architecture ensures robust and reliable biometric authentication while finding applications in various domains beyond biometrics.

**1.7 Code and Dataset:**

Data Loading and Preprocessing

Uses a more detailed directory structure: 1\_Fingerprint, 2\_Iris\_left, and 3\_Iris\_right for each person, with images named sequentially.

Enhanced error handling:

Prints warnings if images are missing or invalid, providing robustness in data loading and helping to identify issues early in the process.

Resizing and Color Conversion

Images are resized to (64, 64) and converted to three-channel (BGR) format using cv2.cvtColor. This step is crucial because the VGG16 model expects three-channel images as input, leveraging pre-trained networks on colored images (ImageNet dataset) for feature extraction.

Feature Extraction

**Pre-trained VGG16 Model**

Employs a pre-trained VGG16 model from Keras, which has been trained on a large dataset (ImageNet). This model extracts high-level, discriminative features from the images, which are expected to be more robust and informative than handcrafted features like LBP and GLCM.

Feature Flattening

Flattens the features extracted by the VGG16 model before further processing. Flattening is essential to convert the multi-dimensional feature maps into a one-dimensional feature vector that can be fed into subsequent dense layers of the network.

Concatenation of Features

Concatenates iris features from both eyes and fingerprint features horizontally to form a combined feature set, ensuring better alignment for model input. This systematic concatenation aligns the features consistently for the neural network, improving the data structure's integrity.

Train-Test Split

Uses train\_test\_split from sklearn to split the dataset. This method is more standardized and reliable, ensuring a reproducible and statistically sound division of the data into training and testing sets.

**Siamese Network Architecture**

Introduces a base network with several dense layers and dropout for regularization. The dropout layers help prevent over fitting by randomly setting a fraction of input units to zero during training, thus promoting generalization.

Concatenated Features

After processing through the base network, concatenates iris and fingerprint features. These concatenated features are then passed through additional dense layers with dropout before the final output layer. This architecture allows for deeper and more complex feature learning, enhancing the model's ability to discriminate between different classes.

Model Training and Evaluation

Increases the number of epochs to 50, allowing the model to learn more effectively over a longer period. More epochs can lead to better convergence and improved performance, provided overfitting is controlled.

Evaluation

Similarly evaluates the model, but with the extended training (50 epochs) and more detailed architecture, likely resulting in better performance metrics. The detailed printing of loss and accuracy during evaluation helps in monitoring and analyzing the model's performance more effectively.

**1.8 Results**

The experimental results demonstrate the effectiveness of the multimodal fusion approach in improving authentication performance compared to single-modality systems. Performance metrics such as accuracy, precision, and recall are presented and analyzed.

`**1.9 Future Advancements**

Model Optimization and Architecture Improvements:

Transfer Learning: Utilize pre - trained deep learning models, such as those trained on large image datasets (e.g., ImageNet), and fine-tune them on the specific task of iris and fingerprint recognition. This can improve feature extraction and reduce training time.

Attention Mechanisms: Incorporate attention mechanisms into the Siamese network to focus on the most relevant parts of the iris and fingerprint images, enhancing the network's ability to distinguish between subtle differences.

Ensemble Methods: Combine predictions from multiple models (e.g., different CNN architectures) to improve overall accuracy and robustness. For example, use an ensemble of CNNs trained on different aspects of iris and fingerprint features.

Multimodal Fusion Enhancements:

Score-Level Fusion: Instead of combining features directly, aggregate the scores (similarity measures) from iris and fingerprint recognition modules. This approach can handle the differences in feature scales and types more effectively.

Decision-Level Fusion: Make independent decisions for iris and fingerprint modalities and then fuse these decisions using a higher-level algorithm, such as majority voting or a weighted decision scheme, to improve reliability.

Scalability and Real-Time Processing:

Edge Computing: Deploy the biometric system on edge devices (e.g., mobile phones, edge servers) to enable real-time processing of iris and fingerprint images. Optimize the models to run efficiently on these devices.

Distributed Systems: Implement a distributed biometric authentication system to handle large-scale data and multiple users simultaneously, ensuring fast and reliable processing in high-demand environments.

Security and Privacy Enhancements:

Template Protection: Implement techniques like biometric cryptosystems or cancelable biometrics to protect stored iris and fingerprint templates, ensuring they cannot be easily reverse-engineered or misused if compromised.

Homomorphic Encryption: Utilize homomorphic encryption to perform computations on encrypted biometric data, allowing the system to verify users without ever exposing their raw biometric information, thus enhancing privacy.

Cross-Domain and Multimodal Integration:

Additional Modalities: Integrate other biometric modalities (e.g., facial recognition, voice recognition) alongside iris and fingerprint to create a more comprehensive and accurate authentication system.

Cross-Domain Learning: Use domain adaptation techniques to make the model robust across different acquisition devices, lighting conditions, and environments, ensuring consistent performance.

1.10 Flaws in the System

Some limitations and challenges of the above proposed idea of biometric system may be:

Computational Complexity:

Processing Power: The fusion of iris and fingerprint data involves complex feature extraction and matching algorithms, which can be computationally intensive. Real-time processing requirements can strain computational resources, especially on mobile or edge devices.

Algorithm Complexity: Developing and tuning advanced algorithms for feature extraction, fusion, and matching can be complex and time-consuming. This includes optimizing parameters for both traditional methods and deep learning models.

Integration and Interoperability:

System Integration: Integrating multiple biometric systems and ensuring seamless operation can be challenging. Compatibility issues between different hardware and software components must be addressed.

Standardization: Lack of standardization in biometric data formats and protocols can hinder the interoperability between different biometric systems and databases.

Security and Privacy:

Data Protection: Ensuring the security of stored biometric templates is critical. Biometric data, if compromised, cannot be changed like passwords. Robust encryption and template protection methods are necessary but can add complexity.

Privacy Concerns: The collection and storage of biometric data raise privacy issues. Users must be assured that their biometric information is securely handled and not misused.

User Acceptance and Usability:

User Cooperation: Biometric systems require user cooperation for data acquisition. Some users may find the process of capturing high-quality iris and fingerprint images intrusive or inconvenient.

User Variability: Variations in user behavior, such as the way they present their finger for scanning or the angle at which they look at the iris scanner, can introduce inconsistencies.

Feature Fusion Challenges:

Feature Heterogeneity: Iris and fingerprint images have different feature characteristics. Finding an effective method to fuse these heterogeneous features without losing important information is challenging.

Evaluation Metrics: Defining appropriate metrics to evaluate the performance of multimodal systems can be difficult. Metrics must consider the trade-off between false acceptance rates (FAR) and false rejection rates (FRR) across modalities.

Benchmarking: Lack of standardized datasets and benchmarks for multimodal systems can make it difficult to compare the performance of different approaches objectively.

Environmental Factors:

External Conditions: Environmental conditions such as lighting, humidity, and temperature can affect the quality of biometric data. For example, dry or wet fingers may produce poor fingerprint images, and ambient lighting can affect iris capture.

Operational Conditions: Multimodal systems need to perform reliably across various operational conditions, including different user demographics and usage scenarios, which adds to the complexity.

Maintenance and Scalability:

System Maintenance: Maintaining and updating multimodal biometric systems can be complex and costly. Ensuring that the system remains secure and performs well over time requires ongoing effort.

Scalability: As the number of users increases, the system must scale efficiently. Managing large databases of biometric data while maintaining fast and accurate matching is a significant challenge.

Legal and Ethical Considerations:

Regulatory Compliance: Adhering to legal regulations and ethical guidelines for biometric data collection, storage, and usage is critical. Non-compliance can result in legal issues and loss of user trust.

Bias and Fairness: Ensuring that the biometric system is fair and unbiased across different demographic groups is essential. Bias in biometric recognition can lead to unequal treatment and potential discrimination.

**CONCLUSION:**

The fusion of iris and fingerprint biometrics represents a significant advancement in the field of biometric authentication. It offers enhanced security, reduced vulnerability to spoofing, and increased reliability across diverse operational conditions. Future work should focus on refining the fusion algorithms, addressing the identified challenges, and exploring the integration of additional biometric modalities to further strengthen the system’s robustness and applicability in real-world scenarios. This project lays a solid foundation for future innovations in multimodal biometric systems, contributing to the development of more secure and user-friendly authentication technologies.