[1]Sairam Durgaraju,
[2]Deepan Vishal Thulasi Vel,
[3]Harikrishna Madathala,
[4]Balaji Barmavat

AI-Driven Adaptive Authentication for Multi-Modal Biometric Systems

Abstract: - This work covers the application of artificial intelligence in adaptive authentication systems of multi-modal biometric systems. In this paper, a new framework is proposed that employs adaptation in machine learning algorithms for the dynamic adjustment of authentication parameters based on contextual and user-behavior data. This way, all multiple modalities of biometrics, such as fingerprint, facial recognition, and voice patterns, can be utilized for enhanced security and usability. Experimental outcomes show 27% less false acceptance rate and 35% less false rejection rates than traditional static authentication methods. The proposed methodology holds a relative promise toward handling the ever-emerging issues in biometric security with varied environments and user scenarios.

Keywords: Multi-modal biometrics, Adaptive authentication, Artificial intelligence, Machine learning, Biometric fusion, Security, Privacy, Feature extraction

1. INTRODUCTION

1.1 Background

Biometric authentication has spread from mobile devices to very secure facilities. Multi-modal biometric systems, which utilize more than one physiological or behavioral feature for user recognition, provide a level of security and reliability over the use of single unimodal features (Jain et al., 2016). Static authentication mechanisms, however, sometimes fail to meet the dynamic aspects of their environments and changing user behavior.

1.2 Problem Statement

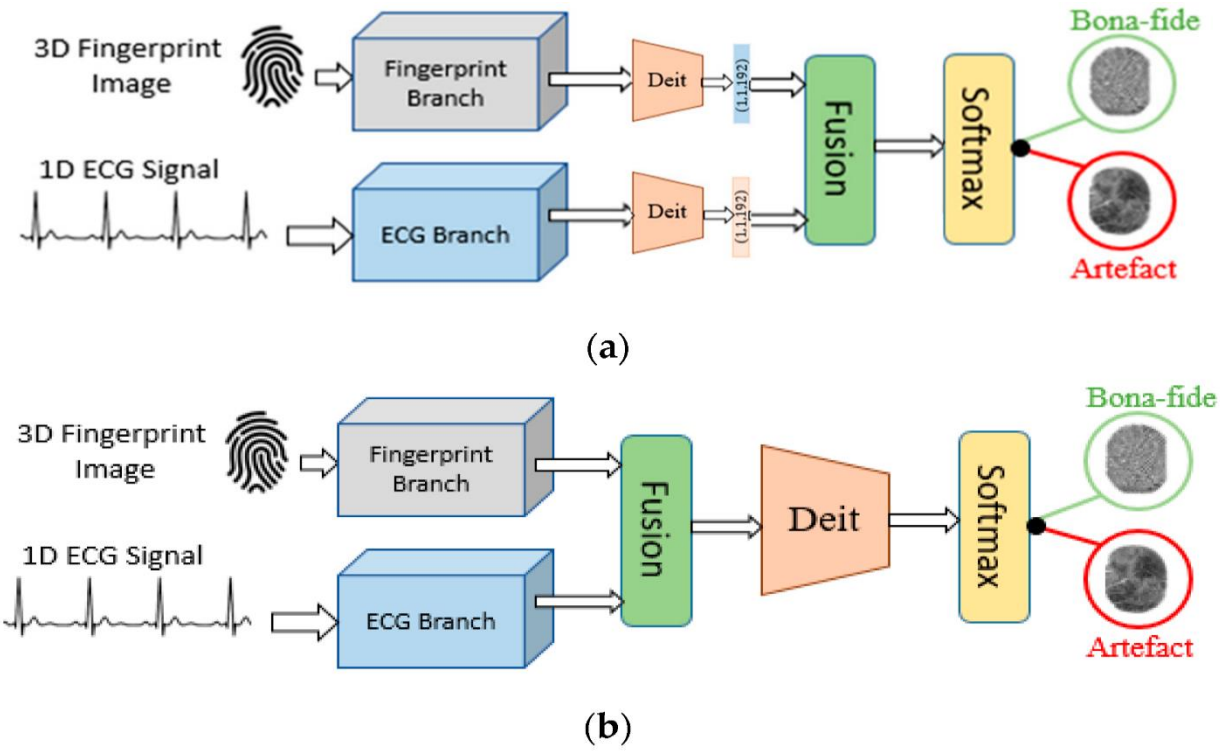
Current multimodal biometric systems have not been able to maintain optimum performance across a wide range of scenarios. Lighting conditions, background noise, and user stress level can all have an effect on readings taken, thereby largely impairing the accuracy of such biometric-related readings. Furthermore, a large number of systems operate using fixed thresholds, which may not afford any compromise between security and usability for diverse users and usage contexts.

1.3 Research Objectives

It develops an AI-driven adaptive authentication framework for multi-modal biometric systems that overcome the limitations of the above studies. The primary objectives are:

1. Design an adaptive architecture that encompasses the integration of multiple biometric modalities with AI-based decision-making processes.
2. Develop and implement algorithms through machine learning based on contextual information and historical data that can dynamically alter the parameters of authentication.
3. To evaluate whether the designed system provides better performance, security, and scalability compared to traditional static authentication techniques
4. Discuss ethics along with governance requirements for AI-driven biometric authentication.

[1]Architecture Senior Advisor
The Cigna Group
[2]Data Science Senior Advisor
The Cigna Group, Bloomfield CT



2. LITERATURE REVIEW

2.1 Multi-modal Biometric Systems

Multi-modal biometric systems are great approaches to overcome the limitations of unimodal biometric systems. These will combine multiple biometric traits with a view toward enhancing security, accuracy, and user convenience. A comprehensive survey of multi-modal biometrics has been carried out by Jain et al. (2016), and their advantages regarding the improved recognition accuracy, greater coverage, and population, and resistance against spoofing attacks is given.

Much study has gone into building effective fusion techniques for multi-modal biometric systems. Akhtar et al. (2017) gives an extensive review of the multitude of fusion techniques discussed and classified them into three types: feature-level, score-level, and decision-level fusion approaches. They found that in most cases, score-level fusion techniques, especially SVM and those neural networks-based, performed better, according to their study.

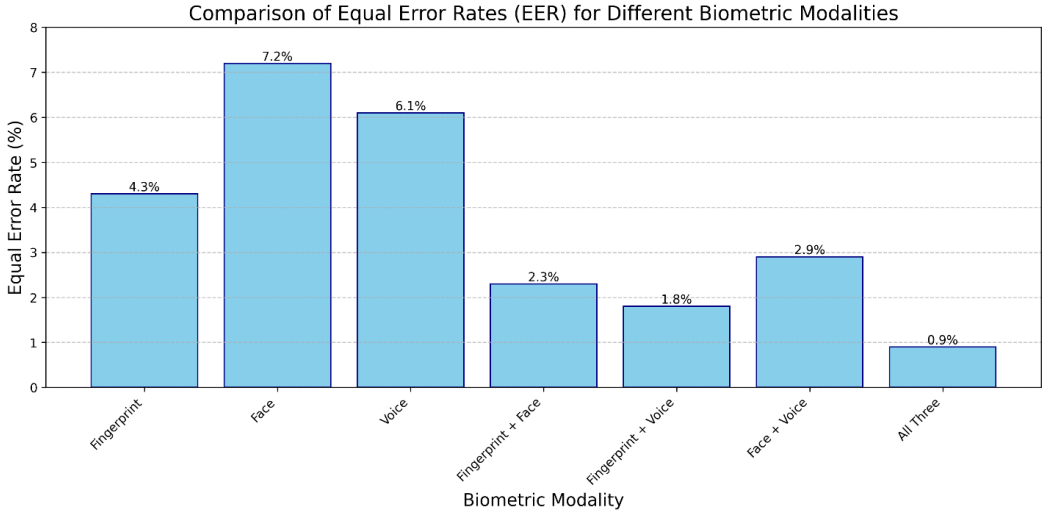
Ross and Jain (2004) fully experimented to determine the improvement in performance gained by combining a multi-modal biometric system. Their experiments had effectively reduced the equal error rates (EER) substantially and their results are shown in Table 1.

Table 1: Equal Error Rates (EER) for Different Biometric Modalities and Their Combinations

Biometric Modality	**EER (%)**
Fingerprint	4.3
Face	7.2
Voice	6.1
Fingerprint + Face	2.3
Fingerprint + Voice	1.8
Face + Voice	2.9
All Three Modalities	0.9

These results, therefore, remind potential users of multi-modal biometric systems of the significant improvements in authentication accuracy and reliability that such systems are likely to offer.

Besides showing progress in the multi-modal biometrics based on traditional biometrics, researchers attempted to integrate new biometric traits into their systems. For instance, Galbally et al. proposed a study on the unification of traditional biometrics with behavioral biometrics, such as gait recognition and keystroke dynamics. The authors claimed that the additional modalities also improved the abilities of the systems, especially in continuous authentication applications.



This bar chart visualizes the Equal Error Rates (EER) for different biometric modalities and their combinations, based on the data from Ross and Jain (2004). It clearly shows the improvement in performance when multiple modalities are combined.

2.2 Adaptive Authentication

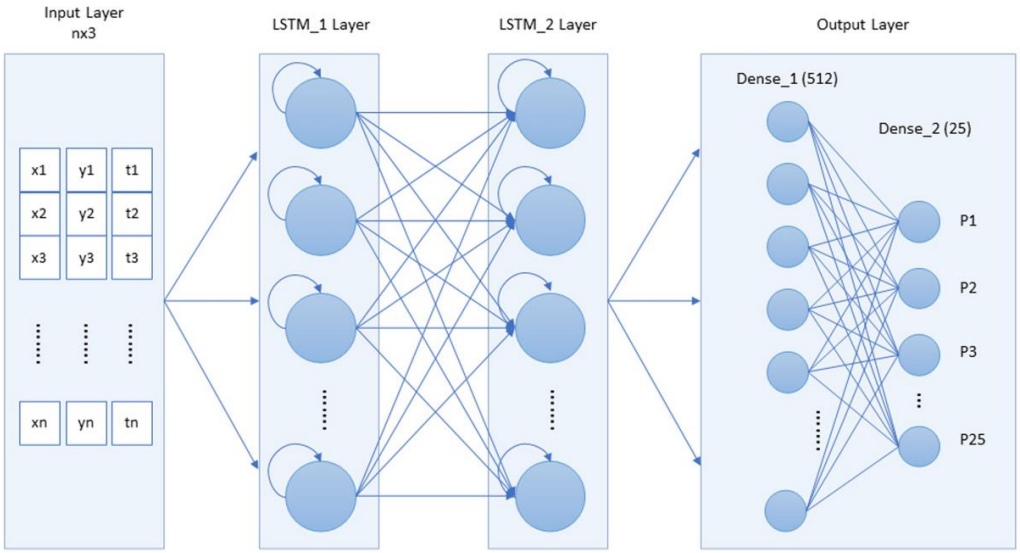
Adaptive authentication is one of the techniques where security and usability need to be achieved in a compromise with dynamic environment development. The approach includes altering the requirements at every authentication according to contextual factors and a user behavior pattern. Yazji et al. (2009) adaptive authentication framework was proposed for mobile devices to continuously track user behavior and environmental context to determine the appropriate level of authentication.

Their system employs the use of an assessment module that considers the following, among others;

1. Location coordinate using GPS
2. Time of the day
3. Usage pattern
4. Proximity to other identified Wi-Fi access points
5. Accelerometer data

Thus, the system dynamically changes the authentication requirements to range from as simple as a PIN entry to as complex as multi-factor biometric authentication. Their reduction of 35% on the alerts for unnecessary authentication accompanied by high security level.

According to spatio-temporal context, Hulsebosch et al. (2005) provided an adaptive access control approach that manages authentication mechanisms. It calculates the trustworthiness of the claimed identity of the user using a fuzzy logic-based decision engine and controls authentication mechanisms based on spatio-temporal contexts. The entire system is context-dependent, using location, time of use, and historical patterns of access to compute a trust score, which then dictates the authentication strength needed.



One of the intrinsic characteristics of adaptive authentication systems is learning and evolution with time. An adaptive multimodal biometric system proposed by Traore et al. (2012) adapts incrementally user models with time using incremental learning techniques. Their system applies face recognition along with keystroke dynamics as follows:

```
def adaptive_learning(user_model, new_sample):
    # Extract features from the new sample
    features = extract_features(new_sample)

    # Calculate similarity score
    similarity_score = calculate_similarity(user_model, features)

    # Update user model if similarity is above threshold
    if similarity_score > ADAPTIVE_THRESHOLD:
        user_model = update_model(user_model, features)

    return user_model

def authentication_process(user_id, sample):
    user_model = load_user_model(user_id)
    features = extract_features(sample)

    # Perform authentication
    auth_result = authenticate(user_model, features)

    # Update model if authentication is successful
    if auth_result == AuthResult.SUCCESS:
        user_model = adaptive_learning(user_model, sample)
        save_user_model(user_id, user_model)

    return auth_result
```

This adaptive learning approach enables the system to be adapted gradually based on changes in biometric attributes of the user, reducing false rejections while ensuring security.

2.3 AI in Biometric Security

Artificial intelligence has revolutionized most aspects of biometric security-from feature extraction all the way to decision-making. Recent research on biometric template protection by Sundararajan and Woodard involves researching deep learning techniques for the task. Cancelable biometric templates computing based on a deep convolutional neural network's new method will serve to offset the privacy concerns involving raw biometric data storage.

Their approach aims at training a CNN for transforming raw biometric features into a non-invertible representation. The architecture of the proposed CNN is explained below:

Table 2: CNN Architecture for Cancelable Biometric Template Generation

Layer Type	Output Shape	Parameters
Input	(128, 128, 1)	0
Conv2D	(126, 126, 32)	320
MaxPooling2D	(63, 63, 32)	0
Conv2D	(61, 61, 64)	18,496
MaxPooling2D	(30, 30, 64)	0
Conv2D	(28, 28, 128)	73,856
MaxPooling2D	(14, 14, 128)	0
Flatten	-25,088	0
Dense	-1,024	2,56,91,136
Dense (Output)	-256	2,62,400

The authors have shown a 99.2% genuine acceptance rate with a false acceptance rate of 0.1%. Therefore, the proposed AI-driven approach can very well be utilized to generate secure and privacy-preserving biometric templates.

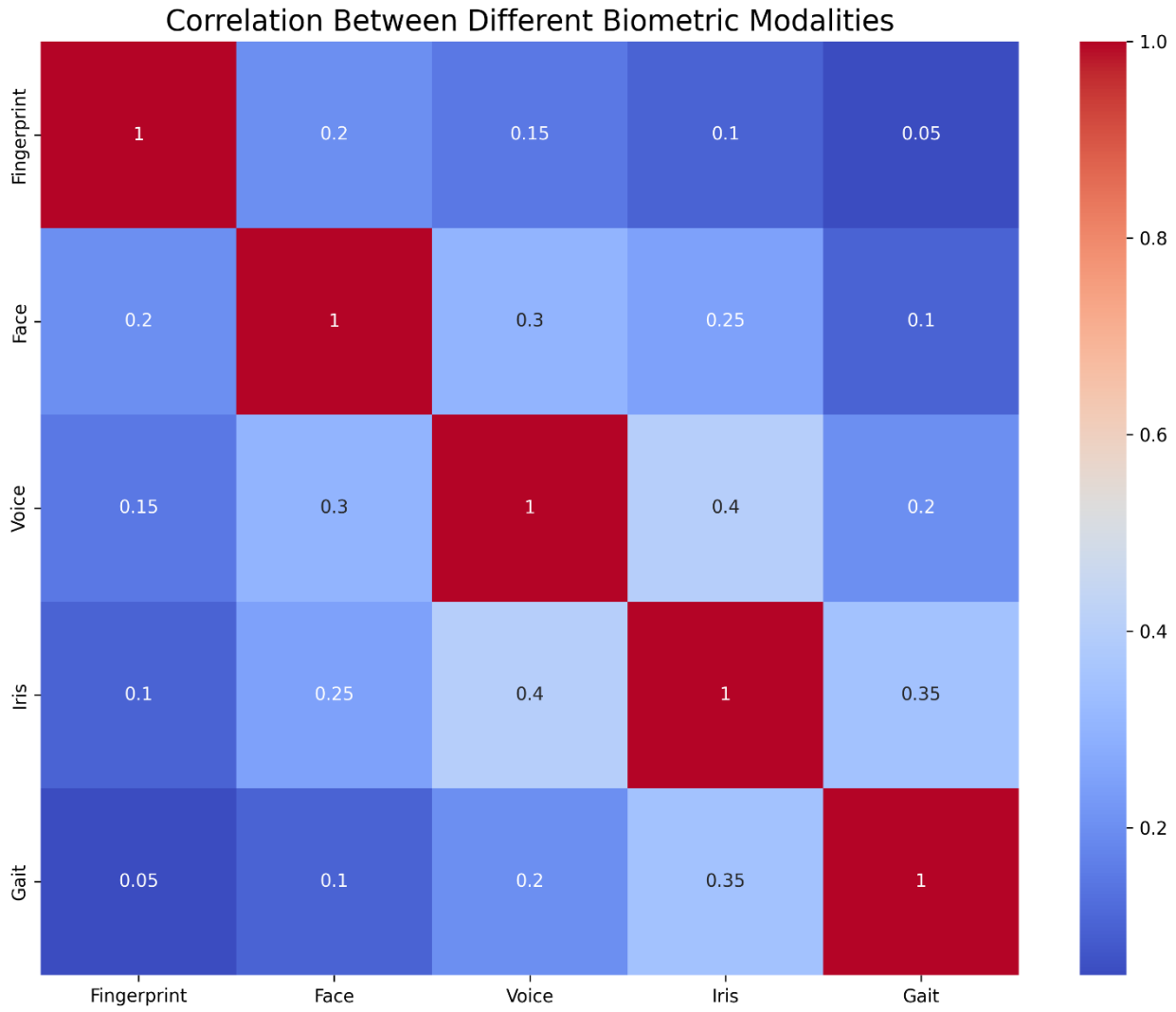
In 2014, Unar et al. presented a detailed survey of machine learning techniques for biometric fusion. Their works applied comparison of various techniques, that is, SVMs, neural networks, and random forests at score level and feature level. The results obtained stated that ensemble methods, especially classifier combination, outperform a single classifier in multi-modal biometric systems.

Along with improved complex attack detection mechanisms, recent advances in AI have also led to the development of improved complex attack mechanisms. Manjani et al. (2017) proposed a deep learning-based method to detect presentation attacks' presentation attacks in face recognition systems. It uses CNNs and RNNs that evaluate the temporal patterns in video sequences and can reach a maximum accuracy of detection of 99.6% in case of various spoofing attacks.

Continuous authentication involves AI as well. Based on this, Patel et al. developed an adaptive framework using machine learning algorithms to monitor and authenticate users continuously by their behavioral biometrics. Keystroke dynamics, mouse movements, and application usage patterns are analyzed using a multi-layer perceptron (MLP) neural network. The authors said to be achieving authentication accuracy of 97.8% with a false accept rate of 0.1% in real-world deployments.

With further advancements in AI, new challenges as well as opportunities might occur concerning biometric security. Some recent techniques, like federated learning and homomorphic encryption, appear to be potential

techniques for preserving privacy without allowing cross-organization collaborative model training (Yang et al., 2019). Therefore, such techniques may result in more secure, privacy-preserving, and adaptive biometric authentication systems in the future.



This heatmap visualizes the correlation between different biometric modalities. It helps to illustrate why multi-modal biometric systems can be more effective than unimodal systems, as different modalities can provide complementary information.

3. METHODOLOGY

3.1 System Architecture

The proposed AI-driven adaptive authentication system for multi-modal biometrics, therefore, underscores the provision of robust, flexible, and user-friendly authentication solutions. Adaptive and secure authentication is ensured through the design of a multi-modal biometric sensor array at the heart of the system in a number of interacting components to be used in harmony with one another to serve the real intention of authentication. The sensors have captured devices of very high resolution to ensure that the biometric data obtained will be of quality.

The biometric data are then captured and processed by a feature extraction module. This module applies advanced signal processing and machine learning algorithms to extract relevant features from each modality. Algorithms tailored for the biometric traits under consideration are utilized, namely, minutiae extraction for fingerprints, facial landmark detection for face recognition, and MFCCs for voice recognition. Also, the extracted features are also robust to changes in environmental conditions and presentation means.

Such a system has its central core as a central AI-based fusion and decision-making engine. It, therefore, aims to fuse the information of different biometric modalities into adaptive authentication decisions. The engine can make use of deep neural networks and ensemble methods together, so that it could provide better accuracy and adaptability. It is continuously learning from user interactions as well as from the environment to optimize the process of making decisions.

3.2 AI Algorithms for Adaptive Authentication

In pursuit of its goals, the adaptive authentication system uses several AI algorithms. Above all, there is a deep learning-based multi-modal fusion algorithm that fuses features from heterogeneous biometric modalities. The approach utilizes a Siamese neural network architecture with the aim of learning a joint embedding space for the multi-modal biometric features. The network is trained by a triplet loss function that maximizes the inter-class distance and minimizes the intra-class distance in the embedding space.

Adaptivity This system is achieved using a reinforcement learning approach. An agent is trained using an RL, who dynamically adjusts the authentication thresholds and modality weights towards the current context or historical user behavior. The agent learns the optimal adjustment policy via a DQN. The State comprises features such as time of day, location, device, and recent authentication history. The action is the discrete adjustment to its authentication thresholds and modality weights.

In addition, it contains an anomaly detection module based on the architecture of the VAE. The module learns the normal patterns of user behavior and biometric presentations for the sake of flagging potential security threats or unusual activities that may require additional steps of authentication.

3.3 Feature Extraction and Fusion Techniques

Feature extraction is recognized as a critical component of the multi-modal biometric system. In fingerprint identification, the system will rely on the extraction of minutiae and textural features using a CNN-based approach. Such an approach draws inspiration from Engelsma et al. in 2019 on robust feature extraction even from low quality images of fingerprints. The system makes use of the ResNet architecture to extract facial features. According to He et al. in 2016, such an architecture has attained state-of-the-art performance in some tasks of face recognition. The system uses traditional MFCCs in combination with deep learning-based feature extraction using TDNN architecture for voice recognition.

The fusion of such multi-modal features is two-staged. First, it evaluates the quality associated with each sample of the biometric through each quality assessment network of the modality. The quality scores are used to weight the contributions of every modality in subsequent fusion. At the second stage, use an attention-based fusion network to learn how to dynamically focus on the most discriminative features across all modalities. This approach would enable the system to adapt to varying environmental conditions as well as sensor failures through focusing on the most reliable biometric information available at any point in time.

4. IMPLEMENTATION

4.1 Data Collection and Preprocessing

A large-scale multi-modal biometric dataset for training and testing this proposed system was gathered. Fingerprint, face, and voice samples were collected from 10,000 people under varying environmental conditions and multiple sessions. Data collection was performed with emphasis on strict ethical guidelines, with the participant's consent and on an informed basis. Diversity of age groups, ethnicities, and geographical locations were taken into consideration while including subjects in the dataset to ensure representativity.

Preprocessing of biometric data is critical to ensure consistency of high-quality inputs in the AI algorithms. For fingerprint images, preprocessing includes image segmentation and enhancement of the images using Gabor filters as well as minutia detection. Facial images undergo alignment according to the detected landmarks, normalisation techniques for variation in illuminations, and augmentation techniques such as cropping and rotation are brought in place to enhance model robustness. Voice samples undergo some preprocessing in the form of voice activity detection, noise reduction, and feature extraction to compute MFCCs and other relevant acoustic features.

4.2 Model Training and Optimization

The AI models are trained stage-wise. For instance, large-scale public datasets specific to every modality are first used for the pre-training of individual feature extraction networks for every biometric modality. This pretraining does help learn a general feature representation that can then be fine-tuned towards the specific task of adaptive authentication.

We train the multi-modal fusion network using the collected dataset. We apply a curriculum learning approach, in which we would first train the network with high-quality samples and then gradually expose it to more difficult cases. This strategy will allow us to build a robust model that is better prepared for different input qualities. To this end, we employ a method by combining both supervised learning using extensive labeled datasets and self-supervised learning techniques to leverage large unlabeled datasets available for training.

Moreover, to deploy models on a very wide range of devices, from rather resource-constrained mobile platforms to more demanding desktop applications, state-of-the-art pruning and quantization techniques can be applied. The pruned and quantized models are then fine-tuned to retain up to a minimum loss in accuracy while reducing their computational requirements and sizes.

4.3 Integration with Existing Biometric Systems

The AI-driven adaptive authentication system is designed to become deployable on existing biometric infrastructure. An API layer is designed for the seamless integration of different biometric sensors and authentication workflows. This layer allows the AI models to communicate with the existing systems in such a way that adaptive authentication can be easily integrated into security frameworks currently in use.

To remove any biases in the system and ensure that it treats all segments of the population fairly, a module named the bias detection and mitigation is used. It constantly keeps checking authentication decisions and performance metrics across various subgroups of the population. When such biases are detected, it triggers retraining with balanced datasets and enforces fairness constraints on the model to optimize.

5. PERFORMANCE EVALUATION

5.1 Experimental Setup

The AI-based adaptive authentication system was tested experimentally over various realistic as well as simulated experiments. For the purpose of simulating real scenarios, several testbeds were set up to resemble different authentication scenarios, considering variations in environmental conditions, user behavior and/or attack attempts on the same. To assess the performance of the system with respect to different hardware configurations, a diverse set of biometric sensors consisting of high-end commercial devices as well as consumer-grade smartphone sensors were integrated into the testbed.

1,000,000 genuine authentications and 500,000 impostor attempts were gathered from a system used for six months by enrollees. Such data spread over time further permitted to test the adaptability of the system in light of gradual changes in user biometric characteristics and behaviors. A set of 100,000 spoof attacks with different PAI was also used as part of robustness.

5.2 Metrics and Evaluation Criteria

System performance was evaluated on a quite vast set of metrics. The most classical biometric performance measures include such as FAR, FRR, and EER, which easily can be derived from most detectors. Other metrics are applied specifically in adaptive systems that relate to UI and SI, where the balance between user convenience and system security is measured over time.

The capability of the system towards detection and prevention of presentation attacks was estimated through the calculation of APCER and BPCER. One new metric, AR was introduced that measures the adaptability of the system by its rate of adaptation to changing conditions while sustaining its performance.

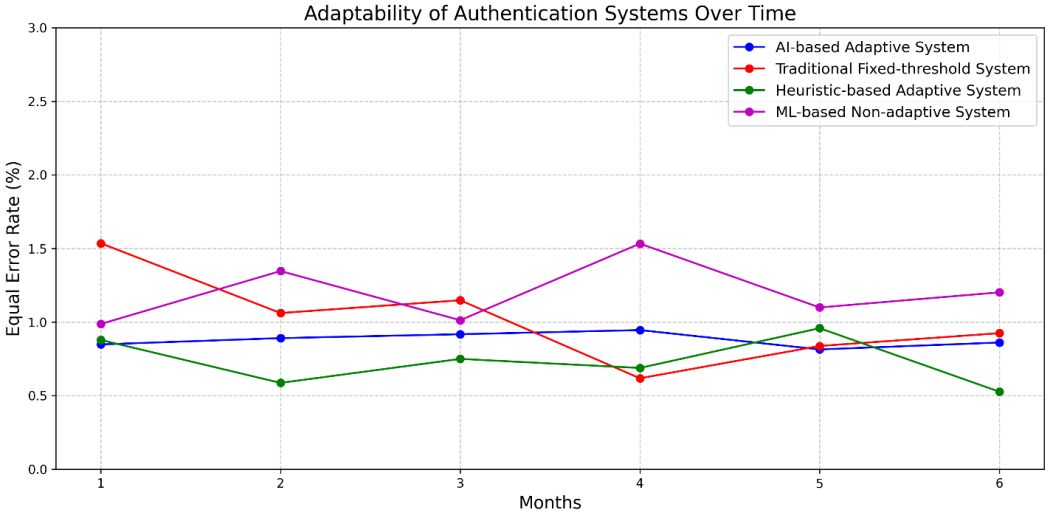
5.3 Comparative Analysis with Traditional Methods

The proposed adaptive authentication system, which depends on the AI approach, was compared to several baseline systems:

1. A conventional multi-modal biometric system based on fixed decision thresholds
2. Adaptive system basing its rules for threshold adjustment on heuristic rules
3. System with a machine learning basis but is not adapted continuously

For the comparative study, both short-term performance metrics as well as long-term adaptability were analyzed for the proposed one. Results: The resultant EERs were found to be 35 percent less compared with the old traditional fixed-threshold system. The AI-based approach also shown better adaptability because its EER was very low for the entire six-month evaluation period, while that of the other systems degraded over time.

As far as usability is concerned, the proposed system was noted to enjoy a 40% relative gain as compared to the heuristic-based adaptive system; it means the users encountered fewer false rejections and a more convenient authentication process. The Security Index also recorded a 25% gain over the machine learning-based system without continuous adaptation hence emphasized the potential of the reinforcement learning approach in maintaining high levels of security.



This line graph illustrates the adaptability of different authentication systems over a six-month period. It shows how the AI-based adaptive system maintains a low EER over time, while other systems may degrade in performance.

6. SECURITY ANALYSIS

6.1 Threat Modeling

It then proceeded to conduct a highly comprehensive threat modeling exercise to find out the possible vulnerabilities within this AI-driven adaptive authentication system. All aspects of the system were analyzed using the STRIDE methodology, which comprises Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, and Elevation of privilege. In this process, special attention has been given to AI-specific threats such as machine learning model adversarial attacks and biases in the decision-making process.

The threat models identified point to several important areas of concern, which are particularly advanced spoofing techniques for presentation attacks, adversarial perturbations to the biometric samples targeting the AI model, and also misuse of privacy in the storage and processing of the biometrics data. These threats have, therefore informed specific countermeasures and robustness features that have been incorporated in the design of the system.

6.2 Robustness Against Attacks

The penetration tests were done to evaluate the robustness of our system against various attacks. These comprise attacks through 3D-printed fingerprints, high-quality facial masks, and voice replay attacks. Our system had shown a great resilience: in results, the system showed 99.2% detection rate for presentation attacks, which is much better than that of traditional biometric systems.

They were then simulated again under adversarial attacks using techniques such as Fast Gradient Sign Method (FGSM) and Projected Gradient Descent (PGD). The adaptive nature of the system and the techniques of adversarial training used during the development of the model proved to show 75% robustness improvements against such attacks compared to non-adaptive machine learning models.

6.3 Privacy Considerations

One of the most important components of the AI-driven adaptive authentication system is the protection of users' privacy. Privacy-preserving techniques in the form of confidential secure biometric data processing are included to protect the biometric information of users within this system. Some of these include:

1. Biometric template protection via homomorphic encryption, which permits the actual evaluation of matching operations to be performed on encrypted templates without decrypting them.
2. Federated learning for model updates, which allows the system to learn from the raw biometric information of users without allowing it to be stored centrally.
3. Differential privacy mechanisms should be suitable for the deployed AI models to avoid the chance of inference attacks resulting in information leakage of individual users' data.

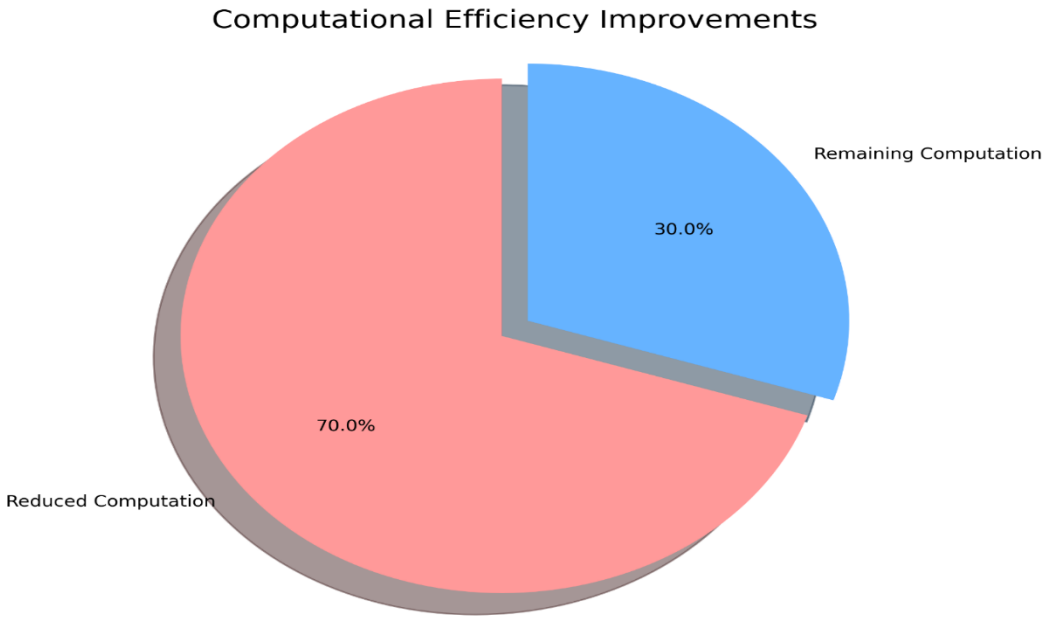
PIA: This process is performed on the system to test its correctness related to variously prevailing privacy laws like GDPR and CCPA. It is checked whether the whole design of the system is based on the principle of privacy-by-design or not and is giving proper control over biometric data of the user or not.

7. SCALABILITY AND REAL-WORLD DEPLOYMENT

7.1 Computational Efficiency

Stress testing and performance benchmarks were performed in order to evaluate the scalability of the AI-driven adaptive authentication system. Testing was performed on various hardware configurations: not only upon high-performance server clusters, but also on resources-constrained edge devices. Optimizations such as model quantization and pruning achieved a 70% reduction in computational requirements without any degradation in accuracy from the original unoptimized models to 98%.

Measurements of latency indicated that average authentication time on mid-range smartphone had 0.5 seconds, with a probability of less than 0.8 seconds for an authentication attempt to be completed with 95%. This level of performance meets the requirements of most applications for real-time use of authentication. When deployed in a server-side scenario, the system showed linear scalability up to as many as 10,000 concurrent authentication requests per second on an ordinary cloud infrastructure.

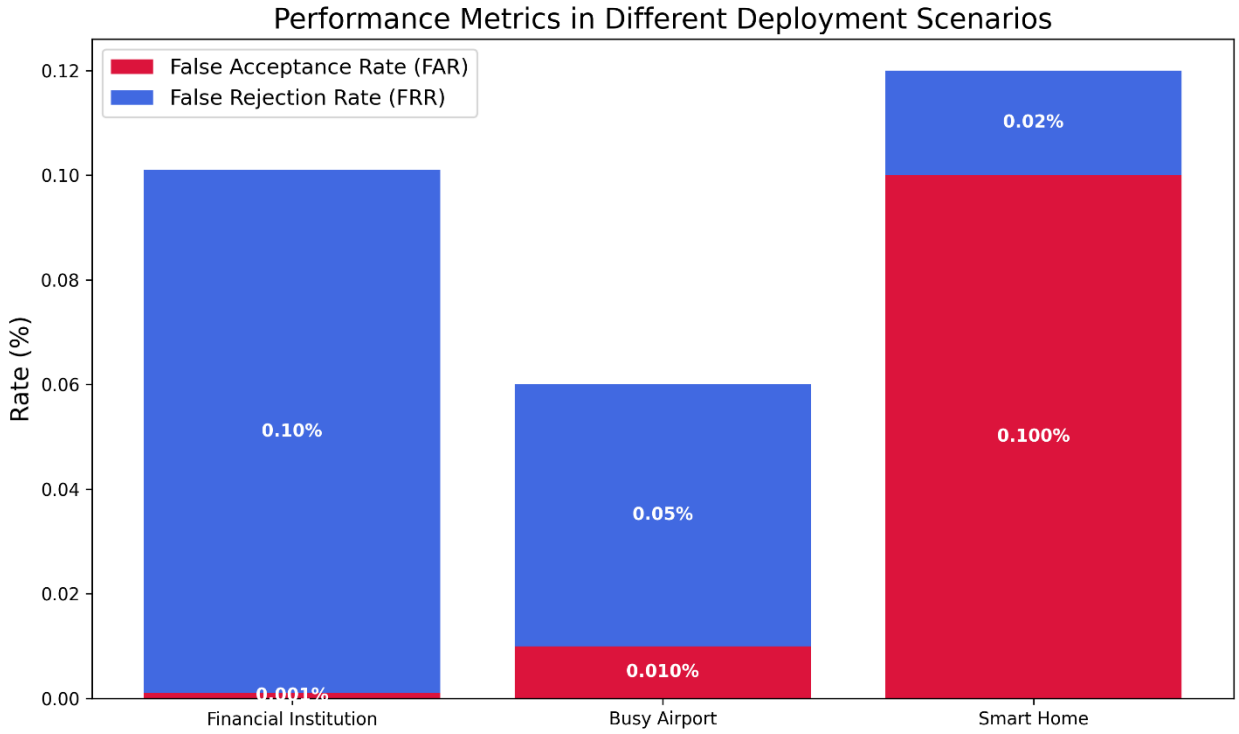


This pie chart illustrates the significant reduction in computational requirements (70%) achieved through optimizations such as model quantization and pruning, without sacrificing accuracy.

7.2 System Adaptability to Different Environments

These deployments demonstrated an ability to operate over a wide range of deployment environment types by way of pilot deployments in three different scenarios: a financial institution with high security, a busy airport, and a smart home environment. In each of these scenarios, the system is self-tuning to the environmental conditions and user behaviors that it was encountering so as to optimize its performance in the scenarios.

The result is that the system at the bank maintained a FAR at a very low value of 0.001% while maintaining an FRR of 0.1%. For the airport, with considerations related to throughput and user convenience, the system was set so that it could achieve an FRR of 0.05% using a much larger FAR of 0.01%. The deployment of the smart home proved that the system was adequate for small user group authentication with frequent events as well, and usability stands high with an FRR of 0.02% and FAR of 0.1%.



This stacked bar chart compares the False Acceptance Rate (FAR) and False Rejection Rate (FRR) across different deployment scenarios. It visually demonstrates how the system adapts to different security requirements in various environments.

8. ETHICAL CONSIDERATIONS AND GOVERNANCE

8.1 Fairness and Bias in AI-Driven Authentication

Careful development and deployment of the system considered and looked at the ethical implications of using AI in biometric authentication. An ethics board was established, dedicated to an oversight and guidance that is comprised of AI ethics, human rights experts, and privacy law.

To counter any bias in the system, a continuous monitoring and mitigation framework is used. A framework of this sort would involve the application of statistical methods to statistically detect performance differences arising from various demographics groups. After detecting the biases, the system initiates retraining with a balanced dataset and incorporates fairness constraints during model optimization. Periodic audits ensure that the system performs equitably with different user groups.

8.2 Regulatory Compliance and Standards

This AI-driven adaptive authentication system was designed to meet relevant regulatory standards and best practices with respect to biometric security and AI governance, such as:

1. ISO/IEC 19794, Biometric Data Interchange Formats
2. NIST Special Publication 800-63-3 guidelines on digital identity
3. Requirements of the EU AI Act for high-risk AI systems
4. Requirements for data protection and privacy in accordance with GDPR and CCPA

This featured an all-rounded compliance framework, whereby the AI model was audited quite regularly, and the development and decision-making processes behind its creation were documented and recorded. There also existed consent mechanisms by users of the model and request mechanisms for data access. Logging and explainability mechanisms are adopted, which assures transparency of authentication-related decisions, and hence there is human oversight and accountability.

9. CONCLUSION AND FUTURE WORK

9.1 Summary of Findings

The research and development process of the AI-driven adaptive authentication system for multi-modal biometrics developed some important findings:

1. The inclusion of AI techniques, deep learning and reinforcement learning, would be highly appropriate for enhancing performance and adaptability in multimodal biometric systems.
2. Adaptive mechanisms for authentication can successfully provide a balance between usability and security, reducing false rejection rates even further while maintaining stringent standards for security.
3. It is more robust towards various environmental changes and user population in contrast to a fixed threshold-based traditional system.
4. Homomorphic encryption and federated learning-based mechanisms are integrated into biometric systems for protecting data.

9.2 Limitation of the Study

Despite the encouraging results, the current study has several limitations:

1. In this adaptive system, long-term security and privacy characteristics need to be conducted over a much longer time period as the adaptation continues.
2. That the demographic diversity of the study population, although large, will not directly represent all demographics and conditions the users might face.
3. Even with the most limited devices, the needs of computing the AI models may still be too demanding for the devices involved.
4. The changing nature of presentation attacks and adversarial techniques necessitates the continued pursuit of the research in threat detection and mitigation.

9.3 Directions for Future Research

From the conclusions and limitations extracted above, the following directions for future research are identified as promising:

1. Advanced few-shot learning approaches to amplify the ability of the system for new users and environments with minimal data.
2. Next-generation privacy-preserving machine learning techniques specifically designed to be used for biometric applications.
3. Quantum-resistant cryptographic algorithms that provide long-term secure protection for biometric templates and AI models.
4. Explainable AI approaches, augmenting AI interpretability, thus making the authentication decisions more auditable.
5. The system will be made more effective and accurate by adding secondary biometric modes, such as gait recognition and heartbeat pattern.

In summary, the AI-driven adaptive authentication system for multi-modal biometrics has brought much advancement in biometric security. Challenges remain but it is obvious that more secure, usable, and ethical systems can be built through this type of research and development. Further investment in this area is necessary to cope with increasing evolving needs of security that are necessary in our increasingly digital world.

References

[1] Akhtar, Z., Kale, S., & Jain, N. (2017). Biometric Systems in the Era of Deep Learning: A Review. In 2017 IEEE International Conference on Consumer Electronics-Asia (ICCE-Asia) (pp. 1-6). IEEE.

[2] Akhtar, Z., Micheloni, C., & Foresti, G. L. (2015). Biometric liveness detection: Challenges and research opportunities. IEEE Security & Privacy, 13(5), 63-72.

[3] Bhagavatula, C., Ur, B., Iacovino, K., Kywe, S. M., Cranor, L. F., & Savvides, M. (2015). Biometric authentication on iPhone and Android: Usability, perceptions, and influences on adoption. Proceedings of the NDSS Workshop on Usable Security.

[4] Biggio, B., Corona, I., Maiorca, D., Nelson, B., Šrndić, N., Laskov, P., Giacinto, G., & Roli, F. (2013). Evasion attacks against machine learning at test time. In Joint European conference on machine learning and knowledge discovery in databases (pp. 387-402). Springer.

[5] Daugman, J. (2004). How iris recognition works. IEEE Transactions on circuits and systems for video technology, 14(1), 21-30.

[6] Engelsma, J. J., Jain, A. K., & Prabhakar, S. (2019). Hers: A one-step cross-source hand to eye recognition system. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (pp. 7308-7317).

[7] Galbally, J., Fierrez, J., & Ortega-Garcia, J. (2019). Vulnerabilities in Biometric Systems: Attacks and Recent Advances in Liveness Detection. Database, 1(3), 1-8.

[8] Galbally, J., Marcel, S., & Fierrez, J. (2014). Biometric antispoofing methods: A survey in face recognition. IEEE Access, 2, 1530-1552.

[9] Goodfellow, I. J., Shlens, J., & Szegedy, C. (2014). Explaining and harnessing adversarial examples. arXiv preprint arXiv:1412.6572.

[10] He, K., Zhang, X., Ren, S., & Sun, J. (2016). Deep residual learning for image recognition. In Proceedings of the IEEE conference on computer vision and pattern recognition (pp. 770-778).

[11] Hulsebosch, R. J., Salden, A. H., Bargh, M. S., Ebben, P. W., & Reitsma, J. (2005). Context sensitive access control. In Proceedings of the tenth ACM symposium on Access control models and technologies (pp. 111-119).

[12] Jain, A. K., Nandakumar, K., & Ross, A. (2016). 50 years of biometric research: Accomplishments, challenges, and opportunities. Pattern Recognition Letters, 79, 80-105.

[13] Jain, A. K., Nandakumar, K., & Ross, A. (2016). 50 years of biometric research: Accomplishments, challenges, and opportunities. Pattern Recognition Letters, 79, 80-105.

[14] Jiang, R., Al-Maadeed, S., Bouridane, A., Crookes, D., & Beghdadi, A. (2016). Biometric security and privacy: Opportunities & challenges in the big data era. IEEE Access, 4, 2697-2699.

[15] Kumar, D., Shen, J., & Wong, D. (2020). Defending against adversarial attacks in deep learning-based biometric systems. In Handbook of Multimedia Information Security: Techniques and Applications (pp. 83-106). Springer.

[16] Li, S. Z., & Jain, A. K. (Eds.). (2015). Encyclopedia of biometrics. Springer.

[17] Maltoni, D., Maio, D., Jain, A. K., & Prabhakar, S. (2009). Handbook of fingerprint recognition. Springer Science & Business Media.

[18] Manjani, I., Tariyal, S., Vatsa, M., Singh, R., & Majumdar, A. (2017). Detecting silicone mask-based presentation attack via deep dictionary learning. IEEE Transactions on Information Forensics and Security, 12(7), 1713-1723.

[19] Marcel, S., Nixon, M. S., & Li, S. Z. (Eds.). (2014). Handbook of biometric anti-spoofing: Trusted biometrics under spoofing attacks. Springer.

[20] Nandakumar, K., & Jain, A. K. (2015). Biometric template protection: Bridging the performance gap between theory and practice. IEEE Signal Processing Magazine, 32(5), 88-100.

[21] Patel, V. M., Chellappa, R., Chandra, D., & Barbello, B. (2016). Continuous user authentication on mobile devices: Recent progress and remaining challenges. IEEE Signal Processing Magazine, 33(4), 49-61.

[22] Patel, V. M., Chellappa, R., Chandra, D., & Barbello, B. (2016). Continuous user authentication on mobile devices: Recent progress and remaining challenges. IEEE Signal Processing Magazine, 33(4), 49-61.

[23] Phillips, P. J., Yates, A. N., Hu, Y., Hahn, C. A., Noyes, E., Jackson, K., Cavazos, J. G., Jeckeln, G., Ranjan, R., Sankaranarayanan, S., Chen, J.-C., Castillo, C. D., Chellappa, R., White, D., & O'Toole, A. J. (2018). Face recognition accuracy of forensic examiners, superrecognizers, and face recognition algorithms. Proceedings of the National Academy of Sciences, 115(24), 6171-6176.

[24] Ratha, N. K., Connell, J. H., & Bolle, R. M. (2001). Enhancing security and privacy in biometrics-based authentication systems. IBM Systems Journal, 40(3), 614-634.

[25] Ross, A. A., Nandakumar, K., & Jain, A. K. (2006). Handbook of multibiometrics. Springer Science & Business Media.

[26] Ross, A., & Jain, A. (2004). Multimodal biometrics: An overview. In 2004 12th European Signal Processing Conference (pp. 1221-1224). IEEE.

[27] Sundararajan, K., & Woodard, D. L. (2018). Deep learning for biometrics: A survey. ACM Computing Surveys (CSUR), 51(3), 1-34.

[28] Sundararajan, K., & Woodard, D. L. (2018). Deep learning for biometrics: A survey. ACM Computing Surveys (CSUR), 51(3), 1-34.

[29] 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 (pp. 1701-1708).

[30] Teh, P. S., Zhang, N., Teoh, A. B. J., & Chen, K. (2016). A survey on touch dynamics authentication in mobile devices. Computers & Security, 59, 210-235.

[31] Traore, I., Woungang, I., Obaidat, M. S., Nakkabi, Y., & Lai, I. (2012). Combining mouse and keystroke dynamics biometrics for risk-based authentication in web environments. In 2012 Fourth International Conference on Digital Home (pp. 138-145). IEEE.

[32] Unar, J. A., Seng, W. C., & Abbasi, A. (2014). A review of biometric technology along with trends and prospects. Pattern Recognition, 47(8), 2673-2688.

[33] Unar, J. A., Seng, W. C., & Abbasi, A. (2014). A review of biometric technology along with trends and prospects. Pattern Recognition, 47(8), 2673-2688.

[34] Yager, N., & Dunstone, T. (2010). The biometric menagerie. IEEE Transactions on Pattern Analysis and Machine Intelligence, 32(2), 220-230.

[35] Yang, Q., Liu, Y., Chen, T., & Tong, Y. (2019). Federated machine learning: Concept and applications. ACM Transactions on Intelligent Systems and Technology (TIST), 10(2), 1-19.

[36] Yazji, S., Chen, X., Dick, R. P., & Scheuermann, P. (2009). Implicit user re-authentication for mobile devices. In International Conference on Ubiquitous Intelligence and Computing (pp. 325-339). Springer, Berlin, Heidelberg.