Automatic Facial Makeup Detection For Device Security Using Machine Learning

|  |  |  |
| --- | --- | --- |
| Atul B. Kathole  Department of Computer Engineering, Dr. D. Y. Patil Institute of Technology Pune, India  atul.kathole1910@gmail.com | Palak Mantri  Department of Computer Engineering, Dr. D. Y. Patil Institute of Technology Pune, India  mantripalak1712[@gmail.com](mailto:sahilraghuvanshi231002@gmail.com) | Shweta Singh  Department of Computer Engineering, Dr. D. Y. Patil Institute of Technology Pune, India  shwetasingh3602@gmail.com |
| Shweta Bodawar  Department of Computer Engineering, Dr. D. Y. Patil Institute of Technology Pune, India  shwetabodawar1302[@gmail.com](mailto:pritigaikwad200217@gmail.com) | Sonali Regude  Department of Computer Engineering, Dr. D. Y. Patil Institute of Technology Pune, India  sonaliregude18@gmail.com |  |

***Abstract*- Significant progress in automated face recognition systems during the last ten years has changed the landscape of security applications. But obstacles still exist, impeding broad adoption, especial-ly in sectors where security is a concern. The impact of non-permanent facial cosmetics on auto-mated face recognition is an important but little-examined topic in this study. To examine the effect of makeup on recognition accuracy, we carefully select two databases: pre- and post-makeup application facial photos. We highlight the possible vulnerability it intro-duces and the pressing need for better understanding by revealing its large effect through exten-sive experimentation. Moreover, we expand our study to include image impersonation detection, a crucial issue for face recognition systems. We create two models: one for spotting makeup and another for telling authentic photos apart from fakes. These models show how to proactively strengthen biometric systems against threats of impersonation. By creating strong algorithmic solutions that can detect image impersonation and navigate hur-dles caused by cosmetics, our study contributes to the integrity and dependability of face recogni-tion systems in security scenarios.**

***Keywords - Facial Makeup Detection, Machine Learning, Device Security, Facial Recognition, Convolutional Neural Networks (CNNs), Transfer Learning, Feature Extraction, Robustness Testing, Authenti-cation, Spoofing Attacks, Image Analysis.***

1. INTRODUCTION

In contemporary society, the integration of facial recognition systems into various security applications has become ubiquitous, offering a potent tool to safeguard sen-sitive information and mitigate unauthorized access. However, the efficacy of these systems can be compromised by external factors, one notable example being the presence of facial makeup. While makeup serves as a common cosmetic enhance-ment, its application can significantly alter an individual's facial appearance, poten-tially impeding the accuracy of automated face recognition.

In response to this challenge, our research aims to investigate the impact of facial makeup on the performance of automated face recognition systems, particularly concerning device security. We recognize that unauthorized access poses a significant threat to the integrity of security systems, and makeup-induced alterations can po-tentially exacerbate this risk. Therefore, our study seeks to comprehensively under-stand the effects of makeup on recognition accuracy and its implications for device security.

Moreover, we acknowledge the importance of developing proactive measures to mitigate the risks associated with makeup-induced alterations. In addition to studying the impact of makeup, we are also developing an imitation detection model aimed at discerning real from fake images. By incorporating this model into our research, we aim to bolster device security by detecting unauthorized access attempts facilitated by altered or fabricated facial images.

Our research is grounded in the recognition of the multifaceted challenges posed by makeup in automated face recognition systems and the imperative to address these challenges to uphold device security. Through a combination of empirical ex-perimentation and algorithmic development, we strive to advance the understanding of makeup's influence on recognition accuracy and devise effective strategies to mitigate its impact.

Ultimately, our research endeavors to contribute to the development of more ro-bust and reliable face recognition systems capable of maintaining device security in the face of evolving threats, including those posed by cosmetic makeup and unau-thorized access attempts. By elucidating the complexities of makeup detection and imitation modeling, we aim to empower security professionals with the tools and insights needed to safeguard critical information and infrastructure effectively.

**Problem Statement :** The project, titled "Automatic Facial Makeup Detection for Device Security Using Machine learning" endeavors to confront the security challenges presented by non-permanent facial makeup and imitation attacks within authentication systems. By integrating machine and deep learning techniques, the project aims to develop a comprehensive solution capable of accurately detecting makeup-applied facial im-ages and discerning between genuine and imitated facial features. This endeavor is paramount for fortifying device security, mitigating risks associated with impersona-tion, and ensuring the integrity of authentication processes in an increasingly digitized landscape.

1. RELATED WORK

C. Chen, A. Dantcheva and A. Ross, "Automatic facial makeup detection with application in face recognition," [1] aimed to develop a method for detecting makeup in facial images to enhance face matching accuracy. They extracted features based on shape, color, and texture, then used a classifier to detect makeup presence. Their work benefits face recognition systems' security and accuracy. Future research could involve testing the method on datasets with male facial images.

Ketan Kotwal, Zohreh Mostaani, and Sebastien Marcel developed a deep learning-based method "Detection of Age-Induced Makeup Attacks on Face Recognition Systems Using Multi-Layer Deep Features " using convolutional neural networks (CNNs) to detect facial makeup, particularly those resembling age-induced changes [2]. Their approach combines color, texture, and shape features for robust makeup detection across different facial regions. This has implications for enhancing privacy and security in applications like face recognition systems and surveillance. Further improvements could focus on real-time and efficient makeup detection algorithms, as well as adaptability to diverse makeup styles and cultural variations.

Mozammel Chowdhury and Junbin Gao "Robust human detection and localization in security applications" [3], in their 2020 IEEE paper, developed a system for extracting facial biometric features using color analysis and fuzzy rules to enhance biometric authentication performance. Their method accurately detects faces by identifying skin color areas using HSV and YCbCr color models, combined with fuzzy rules. This approach, focusing on frontal views in color images, is well-suited for applications like biometric authentication. Future improvements could involve incorporating deep learning techniques to handle variations in facial expressions, angles, and occlusions.

Sanaz Rasti and Mehran Yazdi [4] "Biologically inspired makeup detection system with application in face recognition", in their 2018 IET paper, aimed to design a system for recognizing makeup from face images. Their approach, inspired by human visual recognition abilities, utilizes biologically inspired features (BIFs) based on wavelet transforms. This method offers versatility for computer vision applications and enhances security. Future work may involve exploring combinations of BIFs to address additional challenges in face recognition, such as facial expressions and illumination changes.

Rathgeb, Christian & Drozdowski, Pawel & Busch, Christoph. (2021). Detection of Makeup Presentation Attacks based on Deep Face Representations. [5], in their 2021 ResearchGate publication, aimed to assess the vulnerability of face recognition systems to makeup presentation attacks and develop a detection system, M-PAD, to distinguish these attacks with low error rates. M-PAD processes both reference and probe images to detect differences indicating makeup presentation attacks, highlighting the significant security risk these attacks pose. The study underscores the potential for further advancements in this field, emphasizing the need for larger and more diverse training databases.

G. Guo, L. Wen and S. Yan, "Face Authentication With Makeup Changes," [6], in their 2014 IEEE paper, aimed to develop a robust face recognition system capable of handling facial cosmetics, including makeup detection, and achieving 80% accuracy on a dataset containing both makeup and non-makeup images. Their approach focuses on makeup-invariant face authentication by learning correlations between images of the same person, despite makeup changes. This innovative approach enhances the reliability of face recognition systems in real-world scenarios, making it highly relevant for security applications. Future work may involve refining the approach to handle diverse makeup variations, integrating deep learning for improved makeup detection, optimizing for real-time applications, and exploring multimodal integration for enhanced authentication in various real-world scenarios.

Theiab Alzahrani, Baidaa Al-Bander, and Waleed Al-Nuaimy "Deep Learning Models for Automatic Makeup Detection" [7] conducted a study on automatic makeup detection using deep learning models. They explored various learning schemes, including supervised and semi-supervised learning, with labelled and unlabelled data. Experiments on multiple makeup datasets revealed that combining convolutional auto-encoder with supervised learning yielded the best detection performance, achieving an accuracy of 88.33% and an area under the ROC curve of 95.15%. These findings demonstrate the effectiveness of integrating different learning strategies and utilizing both labelled and unlabelled data for makeup detection, with potential applications in the beauty industry.

Mei Ma and Jianji Wang "Multi-View Face Detection and Landmark Localization Based on MTCNN" [8], in their 2019 IEEE paper, developed a robust method for multi-view face detection and facial landmark localization using Multi-Task Cascaded Convolutional Networks (MTCNN). Their approach trained face detectors for face/non-face classification, bounding box regression, and facial landmark localization, achieving high accuracy in complex environments. The method's comprehensive training approach improves face detection and localization accuracy, making it valuable for applications in computer vision, facial recognition, and human-computer interaction. Future work may focus on optimization through deep learning techniques and real-world applications like surveillance and augmented reality.

Muthukrishnan Ramprasath and M. Vijay Anand [9], in their paper "Image Classification using Convolutional Neural Networks," addressed the challenging task of automatic image classification in the field of computer vision. They highlighted the limitations of existing classification systems and proposed a deep learning approach using Convolutional Neural Networks (CNN). Their system utilized the MNIST dataset as a benchmark for classifying grayscale images. Through training the images using CNN, they achieved a high accuracy of 98%, demonstrating the effectiveness of their model in image classification tasks.

Ahmed Gdoura, Markus Degünther, Birgit Lorenz, and Alexander Effland [10], in their paper titled "Combining CNNs and Markov-like Models for Facial Landmark Detection with Spatial Consistency Estimates," proposed a lightweight hybrid model for facial landmark detection, specifically targeting pupil region extraction. Their model combines a convolutional neural network (CNN) with a Markov random field (MRF)-like process trained on 17 carefully selected landmarks. It achieves state-of-the-art performance on popular facial landmark datasets and effectively filters out spatially inconsistent predictions, demonstrating its accuracy and efficiency in facial landmark detection.

Yuchen Zhang, Yifei Xu, Jiamin Zhao, and Tianjing Du [11], introduced an automated method for 3D facial soft tissue landmark prediction in dentistry. Their neural network architecture directly predicts landmarks from 3D facial models, achieving a mean error of 2.62 ± 2.39 mm, surpassing other algorithms. Over 72% of test data errors fall within ±2.5 mm, and 100% within 3 mm. This method predicts 32 landmarks, demonstrating its accuracy and feasibility for direct use with 3D models in dentistry.

Xuxin Lin and Yanyan Liang [12] propose a Region-Aware Deep Feature-Fused Network (RDFN) for robust facial landmark localization. RDFN addresses the challenge of facial region initialization by combining a region detection subnetwork and a region-wise landmark localization subnetwork. It employs feature fusion schemes to enhance context capture and achieves competitive performance with NMEs of 3.28%, 1.48%, and 3.43% on the 300W, AFLW, and COFW datasets, respectively.

Zahid Akhtar [13] presents a concise survey titled "Deepfakes Generation and Detection: A Short Survey," examining the rise of deepfake technology. The paper outlines the accessibility of face editing apps and their impact on face recognition systems. It provides an overview of recent advances in deepfake techniques, covering identity swap, face reenactment, attribute manipulation, and entire face synthesis, along with both generation and detection methods. Despite progress, an ongoing battle persists between deepfake creators and detection developers. The paper concludes by discussing open challenges and future research directions in this field.

In conclusion, the advancement of automated facial makeup detection systems represents a significant stride in bolstering device security in the digital era. Through the integration of machine learning and deep learning technologies, these systems offer a promising solution to the challenges posed by makeup alterations in authentication processes. However, lingering concerns persist regarding privacy implications, technical feasibility, and ethical considerations surrounding the deployment of such systems. Achieving a delicate balance between effectiveness and ethical implementation remains paramount as we navigate the evolving landscape of device security and authentication mechanisms.

Our proposed model for automatic facial makeup detection for device security harnesses state-of-the-art methodologies to fortify authentication systems against impersonation threats. By leveraging machine learning algorithms and image processing techniques, our model aims to accurately detect makeup alterations in facial images and discern between genuine and imitated features. Additionally, advanced measures such as real-time analysis of facial landmarks, object recognition, and robust facial verification protocols are integrated to ensure comprehensive assessment of user authenticity. Through the fusion of these innovative elements, our model endeavors to address the challenges highlighted in the literature, paving the way for a secure and trustworthy authentication framework in the digital landscape.

1. PROPOSED APPROACH

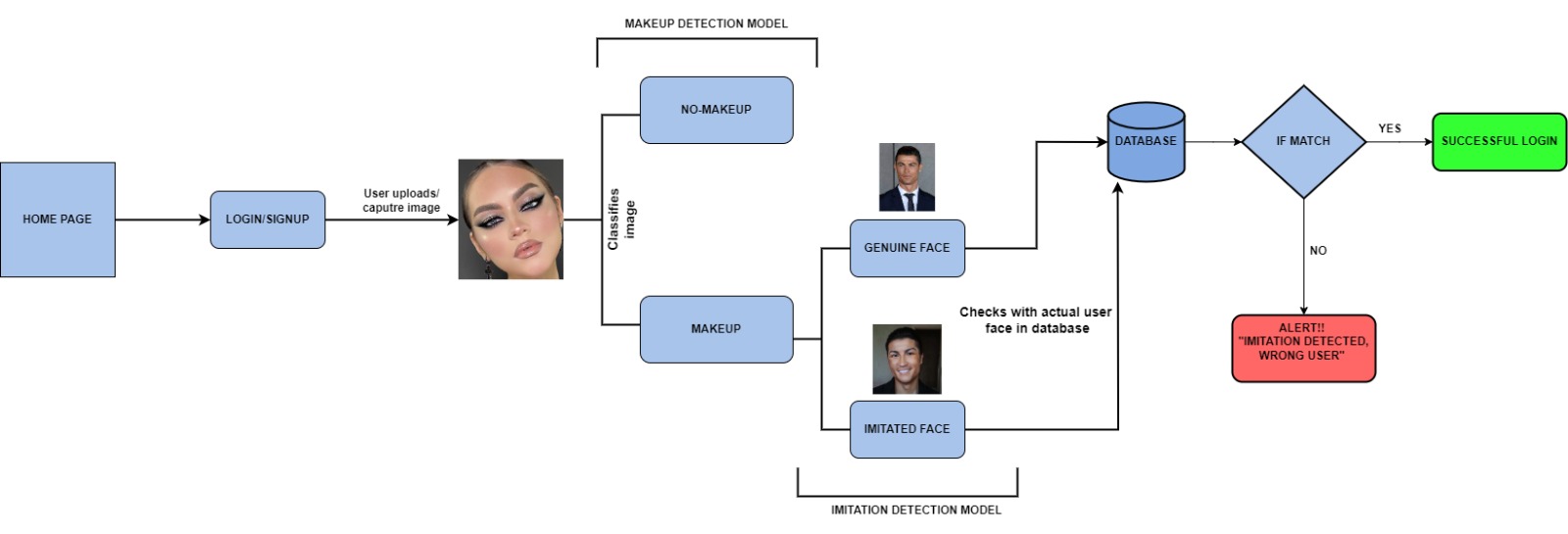


Figure 1: Architecture Diagram

Figure 1 depicts architecture of our proposed approach aims to integrate automatic makeup detection and imitation detection into authentication systems to enhance device security. The system workflow begins with users uploading or capturing their facial images for authentication purposes during registration or login processes. Upon submission, the system utilizes facial detection and landmark detection techniques using MediaPipe and OpenCV to identify and extract key facial features.

Following facial detection, the system proceeds to detect the presence of makeup on the captured facial images using TensorFlow Convolutional Neural Networks (CNN) with the Adam optimizer and activation functions. Leveraging machine learning algorithms and image processing techniques, the system analyzes the facial features to determine whether makeup has been applied.

Simultaneously, the system employs binary classification techniques for makeup detection, where a trained CNN model distinguishes between makeup-applied and makeup-free facial images. This classification process helps identify potential alterations in the user's appearance that may compromise authentication accuracy.

Upon detecting the presence of makeup, the system further scrutinizes the authenticity of the makeup-applied images using advanced image authentication algorithms. TensorFlow CNN models, coupled with the Adam optimizer and activation functions, compare the captured images against a database of genuine facial images to discern whether the makeup-applied images are genuine or imitated.

To facilitate seamless integration and user experience, the system is designed with a user-friendly interface that guides users through the authentication process, the system utilizes alert messages to provide immediate feedback during the authentication process. In cases where makeup is detected or authentication fails, users receive clear and concise alert messages guiding them on the next steps to take, ensuring transparency and assisting users in navigating potential challenges seamlessly.

1. DATASET PREPARATION

In recent years, with the urge of interest in makeup techniques and transformations showcased on social media platforms, the need for comprehensive datasets for makeup detection and imitation detection has become increasingly apparent. However, existing publicly available datasets often lack the diversity and scope necessary to address these specific tasks effectively. To fill this gap, we present two unique datasets meticulously curated from various online sources, catering to makeup detection and imitation detection tasks.

1. Makeup Detection Dataset: Our makeup detection dataset comprises two distinct directories: one containing images of individuals with makeup applied, and the other with individuals devoid of makeup. The images were sourced from a variety of platforms including Instagram, Pinterest, Google, and YouTube makeup tutorials. This dataset is designed to facilitate the training and evaluation of algorithms aimed at detecting the presence or absence of makeup on human faces.



(a) (b) (c) (d)

Figure 2: Example images of individuals from Makeup Detection Dataset. (a) and (c) depicts the individuals without makeup, whereas, (b) and (d) shows individuals wearing makeup.

1. Imitation Detection Dataset: The imitation detection dataset encompasses two categories of images: genuine images and imitated images. Genuine images represent authentic photographs of individuals, while imitated images are synthetic or digitally altered representations attempting to mimic the appearance of the genuine images. Similar to the makeup detection dataset, images for this dataset were gathered from diverse online platforms including social media channels and makeup tutorial videos. This dataset serves as a valuable resource for developing algorithms capable of distinguishing between genuine and imitated facial appearances.

Figure 3: Example images of individuals from Imitation Detection Dataset. (a) and (c) depicts the genuine images, whereas, (b) and (d) shows imitated images.

(a) (b) (c) (d)

Dataset Details:

Makeup Detection Dataset:

* Consists of two directories: one for makeup-applied images and one for non-makeup images.
* Images sourced from Instagram, Pinterest, Google, and YouTube makeup tutorials.
* Each directory contains a diverse range of images representing varying makeup styles, intensities, and facial expressions.

Imitation Detection Dataset:

* Divided into two categories: genuine images and imitated images.
* Genuine images feature authentic photographs of individuals.
* Imitated images encompass digitally altered or synthetic representations attempting to replicate the appearance of genuine images.
* Images gathered from a multitude of online sources, ensuring diversity and variability.

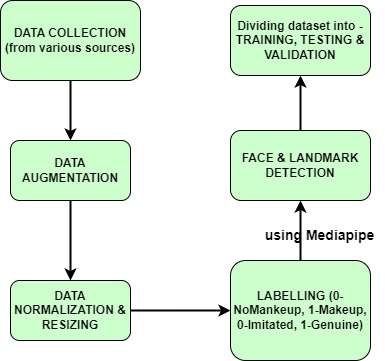


Figure 4: Dataset Preparation

1. ALGORITHMIC OVERVIEW
2. Face detection (OpenCV) :

OpenCV (Open Source Computer Vision) is a popular open-source library for computer vision and image processing tasks. It provides functions and utilities for capturing images from webcams, video files, or image files.

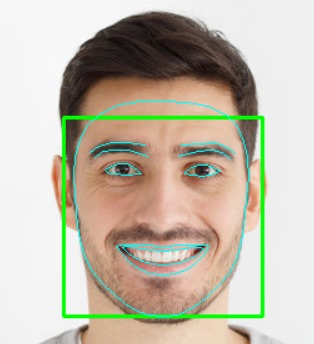
OpenCV provides a wide range of functions and algorithms for image processing, such as filtering, thresholding, edge detection, and morphological operations. These operations are typically implemented using mathematical formulas and algorithms specific to each function.

Mathematical Expression:

1. Convolution Operations : The convolutional kernel is applied to the input image using techniques such as those provided by MediaPipe Face Mesh and OpenCV to generate the output feature map
2. Thresholding: Following convolution, a threshold is applied to determine the validity of the detected face. If the confidence score exceeds this threshold, the detection is accepted; otherwise rejected.
3. Landmarks Localization (Mediapipe) :

MediaPipe Face Mesh provides a pre-trained machine learning model that accurately detects and tracks facial landmarks in real-time from video frames or images. These landmarks represent key points on the face, such as the eyes, nose, mouth, and eyebrows.

The MediaPipe Face Mesh algorithm utilizes a combination of convolutional neural networks (CNNs) and regression techniques to predict the coordinates of facial landmarks. These CNNs are trained on large datasets containing images with annotated facial landmarks, enabling the model to learn to accurately localize landmarks from input images.

(a) (b)

Figure 5: (a) and (b) depicts the face images before and after face and landmarks detection respectively.

Mathematical Expression:

1. Regression Model: Utilizing algorithms such as MediaPipe Face Mesh and OpenCV, facial landmark detection involves predicting the coordinates of key points on the face with a regression model

,

where denotes the model parameters and represents the input image.

1. Spatial Relationship: Spatial relationships between facial landmarks, such as eye spacing or mouth width are identified using MediaPipe Face Mesh and OpenCV.
2. Distance: The Euclidean distance between two facial landmarks and is calculated using techniques provided by MediaPipe Face Mesh and OpenCV:
3. TensorFlow :

TensorFlow serves as a conduit for translating complex mathematical operations into actionable insights, facilitating the creation of sophisticated neural network architectures. In our context, TensorFlow enables the construction of convolutional neural networks (CNNs) that excel at discerning subtle makeup variations on facial features. Through TensorFlow's expressive APIs like Keras, we articulate the intricate interplay of layers, activation functions, and optimization algorithms, shaping the neural network's ability to discern makeup patterns with precision.

Functionality: For makeup detection, TensorFlow's functionalities enable us to preprocess image data, train convolutional neural network (CNN) models, and optimize model parameters using advanced optimization algorithms like Adam.

We leverage TensorFlow's extensive collection of pre-trained models and high-level APIs such as Keras to customize and fine-tune models tailored specifically for detecting makeup alterations in facial images.

Through iterative training cycles, TensorFlow enhances the model's ability to discern subtle makeup cues, ensuring reliable detection performance even in diverse lighting conditions and facial orientations.

Similarly, for imitation detection, TensorFlow empowers us to preprocess image data and train models capable of identifying genuine facial expressions from imitated ones.

Mathematical Expression:

1. Equation for Model Prediction: Let represent the predicted output (i.e., whether makeup is detected or not) for a given input image . In binary classification tasks like makeup detection, the output can be represented as a probability score between and 1, indicating the likelihood of makeup presence.

This can be expressed as:

where represents the neural network model with parameters , and denotes the input image features.

1. Loss Function: The loss function measures the discrepancy between the predicted output and the ground truth label during model training. In binary classification, a common loss function is binary cross-entropy.

The binary cross-entropy loss can be defined as:

where is the number of samples, is the ground truth label (0 or 1), and is the predicted probability.

1. Optimization Algorithm: TensorFlow provides various optimization algorithms for training neural networks, such as the Adam optimizer. The optimizer adjusts the model parameters iteratively to minimize the loss function.

The parameter update rule for the Adam optimizer can be expressed as:

where is the learning rate, , and are the first and second moments of the gradients, and is a small constant to prevent division by zero.

1. Convolutional Neural Network (CNN) :

In the realm of deep learning, CNN stands out as the most renowned and widely utilized algorithm. Unlike its predecessors, CNN has the advantage of autonomously identifying pertinent features without human intervention. Its applications span various domains such as computer vision, speech processing, and face recognition.

CNN's architecture draws inspiration from the neurons found in human and animal brains, akin to traditional neural networks.

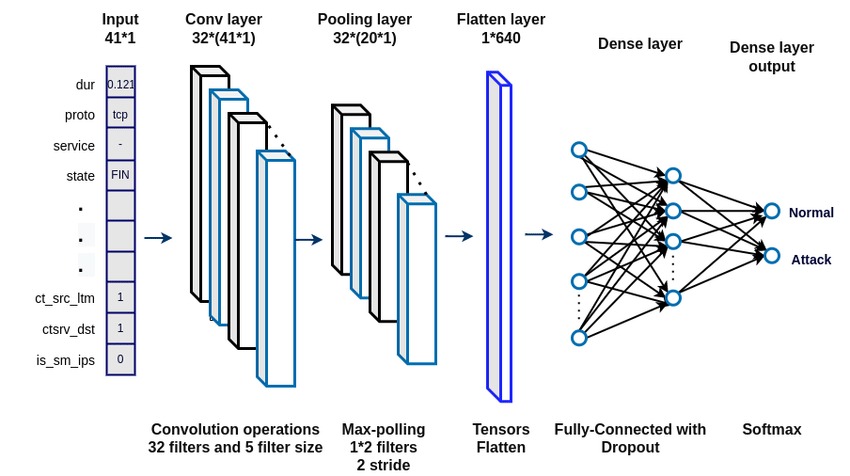


Figure 6: CNN Architecture

1. Convolutional Layer:

Convolutional layers are the backbone of CNNs, designed to extract features from input images. They comprise learnable filters that convolve across the input image, capturing spatial patterns and hierarchies.

Functionality: Convolutional operations in the model detect local patterns such as edges, textures, and shapes, enabling the network to learn discriminative features relevant to makeup detection.

Simulation: During training, these layers convolve over input images, applying learned filters to extract features that contribute to distinguishing genuine and imitated makeup instances.

Mathematical Expression:

1. Output Size Calculation:

where is the output size, is the input size, is the filter size, is zero padding, and is the stride.

1. Convolution Operation:

where is the output feature map,

is the input image,

is the convolutional kernel, is the bias term and is the activation function.

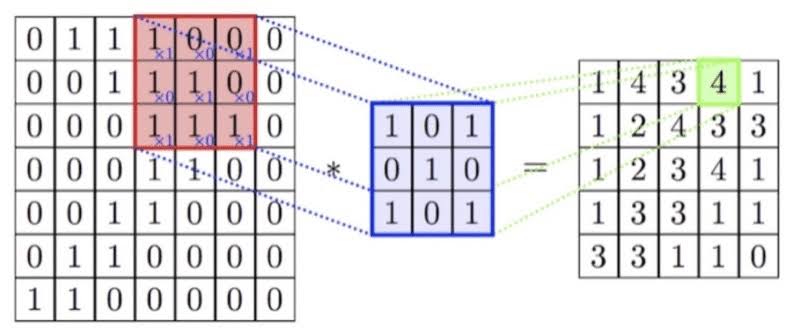


Figure 7: Calculation process of a filter in convolutional layer

1. Max Pooling Layer:

Max pooling layers downsample feature maps, reducing spatial dimensions while retaining important information. They enhance computational efficiency and introduce translation invariance.

Functionality: Max pooling helps in reducing the computational burden by reducing the size of feature maps, thereby extracting the most salient features from the input.

Simulation: Max pooling is applied after convolutional layers, downsampling feature maps by selecting the maximum value within each pooling window.

Mathematical Expression:

1. Average Pooling:
2. Max Pooling:

where is the pooling window size.

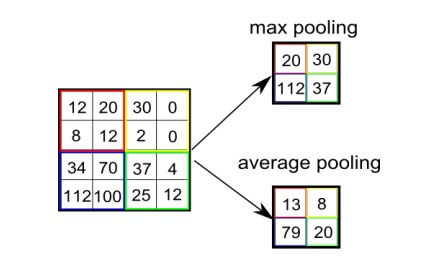


Figure 8: A comparison of max-pooling with average-pooling.

1. Flatten Layer:

The Flatten layer transforms the multi-dimensional output of convolutional layers into a one-dimensional vector, preparing it for input into the fully connected (Dense) layers.

Functionality: Flatten layers reshape the feature maps into a linear array, allowing the subsequent dense layers to process the extracted features.

Simulation: Flatten layers are typically placed after the last convolutional layer, preceding the dense layers.

Mathematical Representation:

Flattening operation involves reshaping the input tensor into a one-dimensional vector without altering the data.

where is the input feature map and is the flattened vector.

1. Dense Layer:

Dense layers, also known as fully connected layers, perform classification based on the extracted features. They connect every neuron in one layer to every neuron in the next layer.

Functionality: Dense layers integrate features learned by convolutional layers to make classification decisions. The final dense layer in binary classification tasks typically has one neuron with a sigmoid activation function.

Simulation: Dense layers process the flattened feature vector, learning complex patterns and relationships to classify input images.

Mathematical Representation:

Dense layers perform matrix multiplication of input features with learnable weights, followed by activation function application.

Output Calculation:

where is the output, is the input vector, is the weight matrix, is the bias vector, and is the activation function.

1. Activation Functions (ReLU & Sigmoid):

Activation functions introduce non-linearity to the model, allowing it to learn complex mappings between inputs and outputs. ReLU and Sigmoid are commonly used activation functions.

Functionality: ReLU (Rectified Linear Unit) introduces sparsity and enables faster convergence by preserving positive values and discarding negative ones. Sigmoid squashes the output between 0 and 1, suitable for binary classification tasks.

Simulation: Activation functions are applied after convolutional and dense layers, introducing non-linearity to the network's output.

Mathematical Representation:

ReLU activation is defined as , while Sigmoid activation is defined as .

1. Adam Optimizer:

Description: Adam optimizer is an adaptive optimization algorithm used to update model weights during training. It combines the advantages of both AdaGrad and RMSProp algorithms.

Functionality: Adam optimizer dynamically adjusts learning rates for each parameter, enabling faster convergence and better performance on non-stationary problems.

Simulation: Adam optimizer is specified during model compilation, governing the optimization process during training.

Mathematical Representation:

Adam optimizer updates model parameters based on the first and second moments of gradients, adjusting the learning rate accordingly.

Parameter Update Rule:

where is the updated parameter, is the current parameter, is the learning rate, and are the first and second moments of the gradients and is a small constant to prevent division by zero.

Situation 1: Normal Behavior

Ground Truth: The user's facial image is captured without any makeup, resembling their usual appearance.

Model Prediction: No anomaly detected (i.e., no makeup detected).

Confusion Matrix:

|  |  |  |
| --- | --- | --- |
|  | Predicted Negative | Predicted Positive |
| Actual Negative | TN (Correct) | FP (False Alarm) |
| Actual Positive | FN (Missed Makeup) | TP (Correct) |

Situation 2: Makeup Anomaly

Ground Truth: The user's facial image is captured with makeup, indicating an anomaly.

Model Prediction: Anomaly detected (i.e., makeup detected).

Confusion Matrix:

|  |  |  |
| --- | --- | --- |
|  | Predicted Negative | Predicted Positive |
| Actual Negative | TN (Correct) | FP (Detected Makeup) |
| Actual Positive | FN (Correct) | TP (Detected Makeup) |

Situation 3: Dual Anomaly (Makeup and Imitation Detection)

Ground Truth: The user's facial image is captured with makeup, and an imitation of the user's face is introduced into the scene.

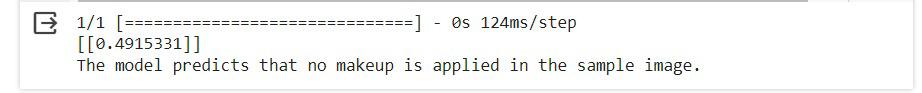
Model Prediction: Anomaly detected (i.e., makeup detected), and imitation detected.

Confusion Matrix:

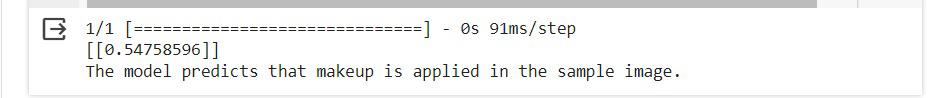
|  |  |  |
| --- | --- | --- |
|  | Predicted Negative | Predicted Positive |
| Actual Negative | TN (Correct) | FP (Detected Makeup) |
| Actual Positive | FN (Missed Makeup) | TP (Detected Makeup and Imitation) |

1. OUTCOMES
2. Makeup Detection

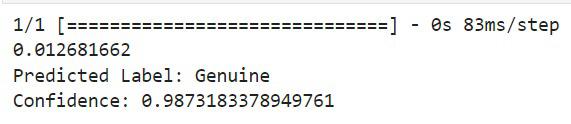




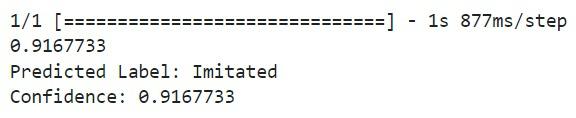




1. Imitation Detection







1. CHALLENGES
2. Privacy Concerns: Ensuring the privacy of individuals while detecting facial makeup can pose challenges, as it involves analyzing personal images and data. Striking a balance between detection accuracy and privacy protection is essential.
3. Technical Limitations: Overcoming technical limitations in image processing and deep learning algorithms to accurately detect subtle makeup variations in different lighting conditions and facial orientations is challenging.
4. Model Robustness: Developing a robust machine learning model that can accurately detect makeup across diverse skin tones, makeup styles, and facial features presents a significant challenge.
5. Real-time Performance: Achieving real-time detection capabilities while maintaining high accuracy requires optimizing model architectures and algorithms for efficient inference on various devices.
6. Dataset Quality and Diversity: Obtaining high-quality and diverse datasets for training the model is crucial. Challenges may arise in collecting sufficient data representing different demographics, makeup types, and environmental conditions.
7. Interpretability and Explainability: Ensuring that the decisions made by the detection system are interpretable and explainable to users and stakeholders is essential for building trust and acceptance.
8. FUTURE SCOPE
9. Increased Accuracy: The accuracy and dependability of facial makeup detection systems may be greatly enhanced by upcoming developments in machine learning and deep learning techniques.
10. Enhanced Robustness: Ongoing research and development initiatives should concentrate on strengthening the detection model's resilience to a range of environmental factors, skin tones, and makeup styles.
11. Real-time Adaptation: To further enhance detection performance, adaptive algorithms that can dynamically adapt to changes in lighting conditions and makeup styles should be used.
12. Privacy-preserving Techniques: Privacy concerns can be addressed while retaining detection accuracy by integrating privacy-preserving techniques like federated learning and differential privacy.
13. Integration with Security Systems: By recognizing people trying to go around security procedures by donning cosmetics disguises, facial makeup detection integrated with current security systems can improve overall security measures.
14. Cooperation and Standards: Establishing best practices and standards for facial makeup detection technology through cooperation with regulatory agencies and industry stakeholders can encourage the technology's morally and responsibly applied applications.

REFERENCES

1. C. Chen, A. Dantcheva and A. Ross, "Automatic facial makeup detection with application in face recognition," 2013 International Conference on Biometrics (ICB), Madrid, Spain, 2013, pp. 1-8, doi: 10.1109/ICB.2013.6612994.
2. K. Kotwal, Z. Mostaani and S. Marcel, "Detection of Age-Induced Makeup Attacks on Face Recognition Systems Using Multi-Layer Deep Features," in IEEE Transactions on Biometrics, Behavior, and Identity Science, vol. 2, no. 1, pp. 15-25, Jan. 2020, doi: 10.1109/TBIOM.2019.2946175.
3. Chowdhury, Mozammel & Gao, Junbin & Islam, Md Rafiqul. (2016). Robust human detection and localization in security applications: Professor Jemal Abawazi and Dr. Rafiqul Islam. Concurrency and Computation: Practice and Experience. 29. 10.1002/cpe.3977.
4. S. Rasti, M. Yazdi, and M. A. Masnadi-Shirazi, “Biologically inspired makeup detection system with application in face recognition,” IET Biometrics, vol. 7, no. 6, pp. 530–535, Nov. 2018.
5. C. Rathgeb, P. Drozdowski and C. Busch, "Detection of Makeup Presentation Attacks based on Deep Face Representations," 2020 25th International Conference on Pattern Recognition (ICPR), Milan, Italy, 2021, pp. 3443-3450, doi: 10.1109/ICPR48806.2021.9413347.
6. G. Guo, L. Wen and S. Yan, "Face Authentication With Makeup Changes," in IEEE Transactions on Circuits and Systems for Video Technology, vol. 24, no. 5, pp. 814-825, May 2014, doi: 10.1109/TCSVT.2013.2280076.
7. Alzahrani, T.; Al-Bander, B.; Al-Nuaimy, W. Deep Learning Models for Automatic Makeup Detection. AI 2021, 2, 497-511. <https://doi.org/10.3390/ai2040031>.
8. M. Ma and J. Wang, "Multi-View Face Detection and Landmark Localization Based on MTCNN," 2018 Chinese Automation Congress (CAC), Xi'an, China, 2018, pp. 4200-4205, doi: 10.1109/CAC.2018.8623535.
9. Ramprasath, Muthukrishnan & Hariharan, Shanmugasundaram & Prasath, Ram. (2022). Image Classification using Convolutional Neural Networks.
10. Gdoura, A.; Degünther, M.; Lorenz, B.; Effland, A. Combining CNNs and Markov-like Models for Facial Landmark Detection with Spatial Consistency Estimates. J. Imaging 2023, 9, 104. <https://doi.org/10.3390/jimaging9050104>.
11. Zhang, Y.; Xu, Y.; Zhao, J.; Du, T.; Li, D.; Zhao, X.; Wang, J.; Li, C.; Tu, J.; Qi, K. An Automated Method of 3D Facial Soft Tissue Landmark Prediction Based on Object Detection and Deep Learning. Diagnostics 2023, 13, 1853. <https://doi.org/10.3390/diagnostics13111853>.
12. Lin, X.; Liang, Y. Region-Aware Deep Feature-Fused Network for Robust Facial Landmark Localization. Mathematics 2023, 11, 4026. <https://doi.org/10.3390/math11194026>.
13. Akhtar, Z. Deepfakes Generation and Detection: A Short Survey. J. Imaging 2023, 9, 18. https://doi.org/10.3390/jimaging9010018.