Augmented Attention: Enhancing Morph Detection in Face Recognition

[1]Katroth Balakrishna Maruthiram
Assistant Professor in CSE
University College of Engineering, Science and Technology,
JNTU Hyderabad
Hyderabad, India

[2]Ranga Muralikrishna
Student
Department of Information Technology
University College of Engineering, Science and Technology,
JNTU Hyderabad
Hyderabad, India

Abstract:- Face Morphing is a technique that involves blending two or more faces to create new often realistic-looking images. These morphed images are generated or created using morphing techniques or photo manipulation tools pose a significant peril to face recognition systems. In this paper, we proposed a method to improve deep learning based face morphing detection systems to be more robust against face morphing attacks. Leveraging deep learning models and algorithms including MTCNN (Multitask Cascaded Convolutional Neural Network) for efficient face extraction from original and morphed faces with a high accuracy and FaceNet for extracting unified embeddings from the faces. The project aims to push the boundaries of face morphing detection capabilities by leveraging feature combination techniques using cosine distance and SSIM(structural similarity index measure) for identifying the similarity between faces and applying spatial attention mechanism which aims to enhance the feature representation learned by the model by focusing on the most informative parts of the image and training support vector machine classifier and voting classifier using the extracted embeddings significantly helps in building a robust face morphing detection system.

Keywords:- *MTCNN, Feature Combination, FaceNet, Attention Mechanism, SSIM, Cosine Distance.*

I. INTRODUCTION

As we know that face recognition systems are employed and deployed in several types of applications and in current days face recognition systems has become an integral part of our everyday life. The face recognition system has been used in a various of applications such as from face unlock feature in smart phone to till very complex and highly secure applications such as border control systems. So, when we consider the face recognition system especially in border control system there is a recommendation from International Civil Aviation Organization (ICAO) to use face biometrics as the primary identifier in the electronic machine readable travel document(eMRTD) such as e-passports. As a result, around 800 million passports deployed with face biometrics around the world.

So as the face biometric system has become prominent in our everyday life, attacks on the face recognition systems also exponentially increased. However, there are several types of attacks on the face recognition systems that can be classified as direct attack and indirect attack. Within the scope of direct attack the most prominent attack type of attack is based on presentation attack. In case face morphing attack, attacker can use two face images to generate a new single morphed image using various tools such as OpenCV, facemorpher, webmorph and stylegan or any deep learning techniques to generate morphed face mages. The main threat is about morphed based attacks are as they are very difficult for both human observer and as well as automated face recognition systems to identify these kind attacks. In the face morphing attack the attacker uses two images for example Let's consider a scenario involving two subjects, Subject1 and Subject2. The attacker performs a morphing operation using images of both subjects to create a morphed subject. Subject1, who is an attacker or thief wanting to escape from border control systems, generates a morphed subject using an image of Subject2, who is innocent, thereby fooling biometric systems.

However, these attacks are a severe threat to the automated face recognition systems. So, this project introduces a robust face morphing detection system by leveraging the deep learning models and feature combination techniques.

A. Objectives and Goals

The ubiquitous goal of the Face Morph Detection System project is to implement a flexible and resilient platform for morph detection systems that converges the following objectives:

- *Training and Dataset Acquisition:*

Collect, Organize and pre-process large-scale datasets suitable for training the machine learning classifiers for face morph detection. The focus is on acquiring morph datasets in which the morphed images are created using various types of techniques, tools and researches such as

- *Tools:*

FaceMorpher and WebMorpher, Techniques: open cv, style GAN and morphs amsl dataset which is generated using morph approach reported in “Extended StirTrace

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24AUG1184

benchmarking of biometric and forensic qualities of morphed face images" [[1]]. The neutral and smiling face images were acquired from "Face Research Lab London (FRLL)" [[2]].

- *Implementation of Deep Learning Models:*

Leveraging MTCNN for efficiently extracting facial features with high accuracy irrespective of the image quality, Face Net for extracting unified embeddings in 512 dimensions which are used in feature combination steps.

- *Leveraging SSIM and cosine distance techniques:*

Utilizing structural similarity index measurement and cosine distance for finding the similarity between two images which can be further helpful to feature combination techniques.

- *Applying Feature Combination and Attention Mechanism:*

The features of the best suitable live images and morphed image are combined. The best suitable images are discovered using the SSIM and cosine distance between images. And then extract embeddings from FaceNet and apply spatial attention mechanism on extracted embeddings.

- *Training Classifiers:*

Train various classifiers such as Support vector machine classifier (SVM), SVM classifier with spatial attention mechanism and ensemble classifier such as Voting Classifier.

- *Performance Evaluation:*

Perform thorough evaluations of the morph detection system's performance using various metrics such as precision, accuracy, resource utilization, confusion matrices and plot the bar graphs using metrics APCER (proportion of attack presentations incorrectly classified as bona-fide presentations), BPCER (Proportion of bona-fide presentations incorrectly classified as attack presentations) and ACER (Average classification error rate)

- *User Interface Design:*

Design a website, It should be user-friendly with easy navigation. Users should find what they need without a hassle. And it'll work great on all devices. Phone, tablet, desktop, whatever. The site adjusts to fit, so users get the same smooth experience no matter what devices they are using.

B. Background

An attacker can easily bypass automated face biometric systems which are installed at airports using sophisticated methods and tools to defeat the biometric system, which is even more important in today's realm of enhanced security. Generating a composite photo, where pictures of two or more people are mixed to create one original image is equally difficult as the face morphing problem. By using this technique, wrongdoers can add some fake ID proofs which may be further used to bypass facial recognition software in border control and other law enforcement areas. We have developed a Face Morph Detection System to address this problem. We intend to use deep learning and computer vision techniques that will provide us with a robust system which can accurately detect genuine images concerning morphed ones. That means that it not only makes biometrics systems more secure, but also provides underlying research and techniques for computer vision and AI.

- *Context:*

Facial Recognition System has been used in wide range of applications from unlock your smartphone till checking person through border control. Nevertheless, the emergence of advanced image synthesis techniques and tools as well as those for face morphing, represent a great risk in terms of fidelity and security to automatic recognition systems based on faces. It is the process of combining two or more facial images in such a way that you do not cannot guess whether it faces one single individual or not. This is a very important security problem that our face morphing detection systems are facing and these problems are solved using advanced machine learning techniques such as deep learning and computer vision. By detecting the morphed images, this system intends to discriminate between original or genuine facial images and those being manipulated by good face editing methods even with very minor changes that is likely unseen in general tasks if you asked for a human observer.

- *Motivation:*

- *Security Enhancement:*

The principal reason certainly is the improvement of security in facial recognition systems used for critical applications, e.g. Border Control and Financial Service or Government Identification. As a result, these services help prevent identity fraud when combined with their popular service that detects morphed images so unauthorized access can be stopped.

- *Technological Advancement:*

The project pushes the boundaries of current face morphing detection techniques by incorporating spatial attention mechanisms and advanced feature extraction methods. This contributes to the broader field of biometric security and computer vision.

- *Adaptability to Evolving Threats:*

As morphing techniques become more sophisticated, there's a pressing need for detection systems that can adapt and improve. Your system's use of machine learning allows it to potentially learn and recognize new morphing patterns over time.

- *Cross-Domain Application:*

While initially focused on security applications, the technology has potential uses in forensic analysis, digital media authentication, and social media content moderation, addressing the broader issue of digital image manipulation.

- *Ethical Considerations:*

The system contributes to the ongoing dialogue about privacy, consent, and the ethical use of facial recognition technologies. By improving the reliability of these systems, it helps balance security needs with privacy concerns.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24AUG1184

➢ *Research Contribution:*

This work adds to the growing body of research in biometric security, potentially opening new avenues for further study in areas such as multi-modal biometric verification and adversarial machine learning in the context of facial recognition.

C. *Case Study*

A German activist pulled a daring maneuver with the Lambda Wars backend and, using face morphing photos of Federica Mogherini, EU High Representative for Foreign Affairs and Security Policy. The activist got a photo of Federica Mogherini and used some next-level face morphing technology to fade it into her own image. This produced a ghostly image that maintained aspects of both faces.

The activist then submitted this altered image to German passport application control. However, as if all the security in place meant nothing, it is hard to believe how a photo could eventually be accepted and then make its way through border controls for her so that she was able obtain a passport with Mogherini's identity. The event clearly highlights the limitations of both biometric systems and human observers in the detection of sophisticated morphed images. This ability of activists (as well as the non-activists) to counter such checks reveal possible weaknesses in current biometric verification methods and imperative evidence for more sophisticated anti-morphing detection.

II. LITERATURE REVIEW

A. *Generation and Detection of Face Morphing Attacks:*

➢ *Methods:*

- *Deep Learning-Based Feature Extractors:*

Researchers have employed deep learning models to extract features from images that can help in distinguishing between genuine and morphed faces. Convolutional Neural Networks (CNNs) are commonly used for this purpose.

- *Image Enhancement Techniques:*

Techniques such as histogram equalization, contrast adjustment, and noise reduction are applied to improve the quality of images before feeding them into the detection models. These enhancements help in highlighting subtle differences between genuine and morphed images.

- *Classifier Models:*

Various classifiers, including Support Vector Machines (SVM), Random Forests, and neural networks, are used to classify images as either genuine or morphed based on the extracted features.

- *Morph-3 Images:*

A novel approach involves the creation of Morph-3 images, which are more realistic and harder to detect. These images are used to train and test the detection models, pushing the boundaries of current detection capabilities.

➢ *Datasets:*

- *Publicly Available Datasets:*

Several publicly available datasets, such as the FRGC (Face Recognition Grand Challenge) and LFW (Labeled Faces in the Wild), are used for training and testing morphing detection models. These datasets provide a diverse range of facial images, which are essential for robust model training.

- *Custom Datasets:*

Researchers also created custom datasets by morphing images from existing datasets. These custom datasets are tailored to specific research needs and help in evaluating the performance of detection models under various conditions.

➢ *Key Findings:*

- *Improved Detection Accuracy:*

The introduction of deep learning-based feature extractors and image enhancement techniques has significantly improved the accuracy of morphing attack detection. Models trained with these methods have shown higher detection rates compared to traditional methods.

- *Challenges with Realistic Morphs:*

Despite advancements, detecting highly realistic morphs, such as Morph-3 images, remains challenging. These images are designed to be more lifelike and can often bypass current detection systems.

B. *Face Morphing Attack Generation and Detection:*

➢ *Methods:*

This comprehensive survey covers various techniques for generating and detecting morphing attacks. It highlights the vulnerabilities in facial recognition systems and the necessity for robust detection algorithms.

➢ *Datasets:*

It evaluates methods using datasets like FERET, FRLL, and others, emphasizing the need for diverse and extensive data for better detection performance.

➢ *Key Findings:*

The survey concludes that while significant progress has been made, the complexity of realistic morphs still poses a challenge, necessitating continuous improvement in detection techniques.

C. *Enhanced Face Morphing Attack Detection using error-level Analysis and Efficient Selective Kernel Network*

➢ *Methods:*

- *Error-Level Analysis (ELA):*

ELA is a technique used to detect discrepancies in the compression levels of different parts of an image. By analyzing the error levels in the R, G, and B color channels, ELA can highlight subtle differences that may indicate

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24AUG1184

morphing. This method is particularly useful for identifying inconsistencies that are not visible to the naked eye.

- *Efficient Selective Kernel Network (ESKNet):*

ESKNet is a deep learning model designed to dynamically adjust its receptive fields to capture crucial features in images. This network can selectively focus on different parts of an image, making it highly effective in detecting morphed faces. The selective kernel mechanism allows the network to adapt to various scales and orientations of features, enhancing its detection capabilities.

➢ *Datasets*

- *Publicly Available Datasets:*

Standard databases such as the FRGC (Face Recognition Grand Challenge) and LFW (Labeled Faces in the Wild) are commonly used for training and testing morphing detection models. These datasets provide a diverse range of facial images, essential for robust model training and evaluation.

➢ *Key Findings:*

- *Enhanced Detection Accuracy:*

The combination of ELA and ESKNet has shown significant improvements in detection accuracy. ELA helps in highlighting subtle differences in the image, while ESKNet's dynamic receptive fields capture these differences effectively. This synergy results in higher detection rates compared to traditional methods.

III. SYSTEM DESIGN

➢ *System Architecture:*

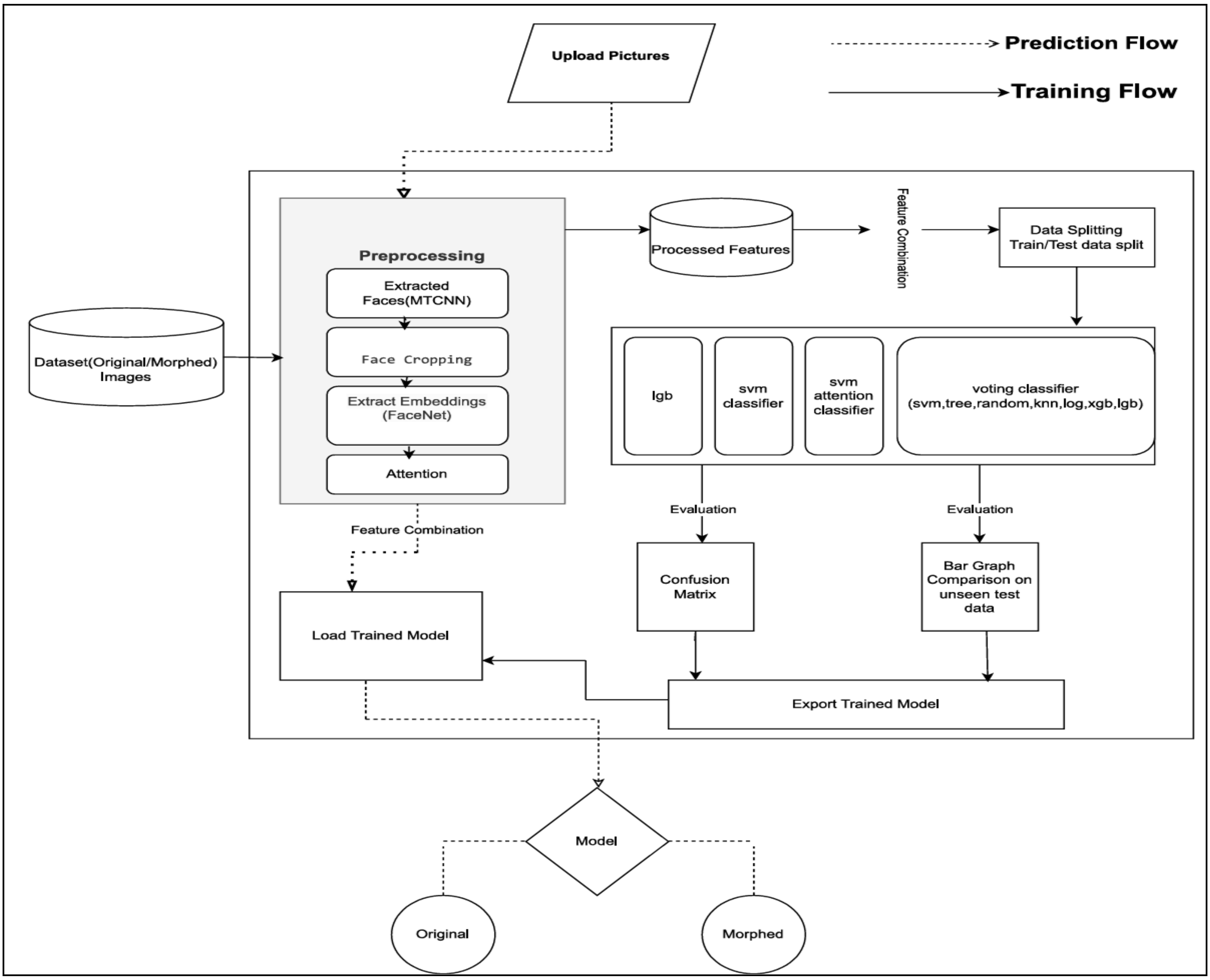

Fig 1 System Architecture

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24AUG1184

➢ *Components Overview:*

- *Dataset Handling:*

The system starts with a dataset containing original and morphed images.

- *Preprocessing:*

✓ *Face Extraction (MTCNN):* Multi-task Cascaded Convolutional Networks (MTCNN) is used to detect and extract faces from the images.
✓ *Face Cropping:* The extracted faces are cropped to focus on the relevant facial features.
✓ *Extract Embeddings (FaceNet):* FaceNet, a deep learning model, generates embeddings (numerical representations) of the faces.
✓ *Spatial Attention Mechanism:* This enhances the feature extraction process by focusing on the most significant parts of the image.
✓ *Feature Combination:* The features extracted from the images are combined to form a comprehensive feature set, which is stored in the "Processed Features" repository.

- *Data Splitting:*

The combined features are split into training and testing datasets to train and evaluate the models.

- *Model Training and Evaluation:*

✓ *Classifiers:* Various classifiers such as SVM (Support Vector Machine), SVM with attention classifier, and a voting classifier (comprising SVM, Decision Tree, Random Forest, KNN, Logistic Regression and XGBoost) are trained using the processed features.
✓ *Evaluation:* The models are evaluated to measure their performance. Evaluation metrics like the confusion matrix are used to understand the accuracy and performance of each classifier.
✓ *Model Export:* The trained models are exported for later use. The bar graph comparisons of performance metrics on unseen test data are generated for better understanding.
✓ *Prediction Flow:* For predictions, the trained model is loaded, and new images can be uploaded. The system preprocesses these images, extracts features, and uses the trained model to classify them as original or morphed.
✓ *Output:* The final output of the system is a classification of the image as either "Original" or "Morphed".

This architecture ensures robust and efficient processing, training, and evaluation of facial images for morphing attack detection. The use of advanced preprocessing techniques, multiple classifiers, and a voting mechanism enhances the system's accuracy and reliability in identifying morphed images.

IV. IMPLEMENTATION

The project utilizes newly introduced models, frameworks, and tools customized to facilitate the development of robust models. At the base, we have used Python due to its simplicity and suitability for developing web applications. Python integrates machine learning and deep learning models easily thanks to its extensive support for predefined models. Flask framework has been used to create website, handles the HTTP requests etc. because it works on few structures and is most convenient for the model communication with simple set up. In simple terms, Flask is a small web framework offering required tools to build everything from simple websites or blogs. It is simple and flexible, making it a great candidate for integrating machine learning models as well as deep learning in web applications. Flask also provides extensions to add additional functionality, such as database support form validation and much more making development neat. MTCNN is used for face extraction due to its high accuracy. For extracting embeddings, we use FaceNet. We combine the features of original and morphed embeddings and train various classifiers to build the model. MTCNN (Multi-task Cascaded Convolutional Networks) excels in detecting faces with high precision and is robust against variations in lighting and angles. FaceNet generates highly accurate embeddings that capture the essential features of the faces. By merging the embeddings from both original and morphed faces, we create a comprehensive feature set. This enriched dataset is then used to train multiple classifiers, enhancing the overall accuracy and reliability of the face morphing detection model.

A. *Training Process*

➢ *Dataset Acquisition and Restructuring:*

Our training process begins with the collection of large datasets, including FRLL (Face Research Lab London) [[2]] and AMSL Morphs [[1]], which contain morphed images based on the FRLL dataset. We also generate morphed images using various tools such as FaceMorpher, FantaMorph, OpenCV, WebMorph, and StyleGAN.

We restructured the dataset to suit our needs. For example, if there is a morphed image, it will be generated using two original images. Our dataset contains multiple folders, each with two subfolders: original and morphed.

Since we have two original images and one morphed image (created by combining the two originals), our approach involves selecting the original image that is most similar to the morphed image using cosine distance and SSIM (Structural Similarity Index Measure). We then extract the features of the best-matching original image and the morphed image. These features are combined and used to train the model.

➢ *Leveraging Cosine Distance and SSIM:*

To select the best matching original image for the morphed image, we use cosine distance and Structural Similarity Index Measurement (SSIM). These two metrics help identify the original image that is closest to the morphed image.

Cosine distance is used to measure the cosine of an angle between vectors, in this context images. It simply measures how similar the images features are, which means on smaller numbers to value that goes higher it will be more similar. It is a measure to assess the similarity of images, by computing

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24AUG1184

contrasts and luminance differences and structure using SSIM. It is a perceptual similarity measure which encapsulates the various possibilities of similarities that might be applicable to images.

By combining these two metrics, we can accurately select the original image that most closely matches the morphed image, ensuring that the training data is optimally structured for model training.

➢ *Extracting Faces using MTCNN:*

This project used MTCNN for pulling out face features. It has shown a lot of accuracy in its detection as well, better than any other model like dlib, OpenCV DNN, Yunet, Pytorch-MTCNN, and RetinaFace. MTCNN is used to effectively extract all face information like bounding box (x, y co-ordinations and height, width of the face) etc. As well as detecting major features like eye locations, the nose and mouth corners.

MTCNN follows a three-stage cascade structure, which consists of the Proposal Network (P-Net), the Refine Network(R-Net) and The Output network(O-net). P-Net finds candidate facial regions, R-Net configures those regions and O-Net finally outputs refined bounding box locations as well as the positions of 5 face landmarks. The multi-stage process guarantees accurate and dependable face detection and feature extraction.

➢ *Extracting Embeddings using FaceNet:*

We used the FaceNet, which is a deep learning model to extract vector embeddings for faces. What FaceNet does is map face to a Euclidean space rather than simply representing as dictionary of IDs (names) and the distance between embeddings reflect similarity of faces. Here, an image is passed as input to a model which contains CNN layers including the convolutional layer, pooling layer and fully connected layers. The goal of this network is to take an image and convert it into a vector, called embedding, that encodes the facial features in some high-dimensional space. During learning FaceNet uses triplet loss where each input image competes against two other images, the anchor (same class as positive) and a negative. Triplets loss makes sure that anchor, and the positive embeddings have smaller distance than a negative embedding which allows us to have very accurate discriminative facial embeddings.

➢ *Spatial Attention Mechanism:*

Applying spatial attention mechanisms to FaceNet-extracted embeddings enhances the feature representation by focusing on critical regions of the embedding. Incorporating attention mechanisms increases the model's accuracy and robustness in detecting morphed images. This approach allows the model to prioritize the most informative parts of the embedding, leading to improved performance in distinguishing between original and morphed images.

➢ *Feature Combination:*

We used a feature combination technique to combine the best-matching original image and the morphed image that is closest to it, as determined by cosine distance and SSIM. First, we extracted the faces and embeddings from these images. Then, we concatenated the embeddings using the numpy module and labeled them as "morph," storing these feature arrays.

Similarly, we performed the same process for all original images and morphed images separately, extracting their features and storing them. This structured approach ensures that our dataset is well-organized, with clear distinctions between original and morphed images, enhancing the accuracy and robustness of our model.

➢ *Training Classifiers:*

In our project, we have trained various classifiers to enhance the detection of morph attacks. We utilized Support Vector Machines (SVM), which are effective for high-dimensional spaces. The voting classifiers incorporate multiple algorithms such as SVM, decision trees, random forests, and k-nearest neighbors (KNN) to improve robustness by combining their strengths. We also employed Extreme Gradient Boosting (XGBoost or XGB), which is known for its performance and speed in handling large datasets with complex patterns. This ensemble approach ensures comprehensive analysis and improved accuracy in detecting morph attacks.

V. EXPERIMENTAL RESULTS

In this section, we discuss how the face detection system performed on various unseen datasets. The model was trained using the FRLL neutral original faces dataset and morphs from the AMSL dataset. For evaluation, the model was tested on the FRLL smiling original dataset and additional datasets including FaceMorpher, WebMorph, FantaMorph, and StyleGAN. The results, which are presented below, demonstrate the model's effectiveness and generalization capability across different types of morphed and original images. This section reports general detection accuracy and utilizes standard metrics for biometric systems as recommended in the document ISO IEC 30107-3 [[5]] including APCER (Proportion of attack presentations incorrectly classified as bonafide presentations) and BPCER (Proportion of bonafide presentation incorrectly classified correctly as attacker's presentation.

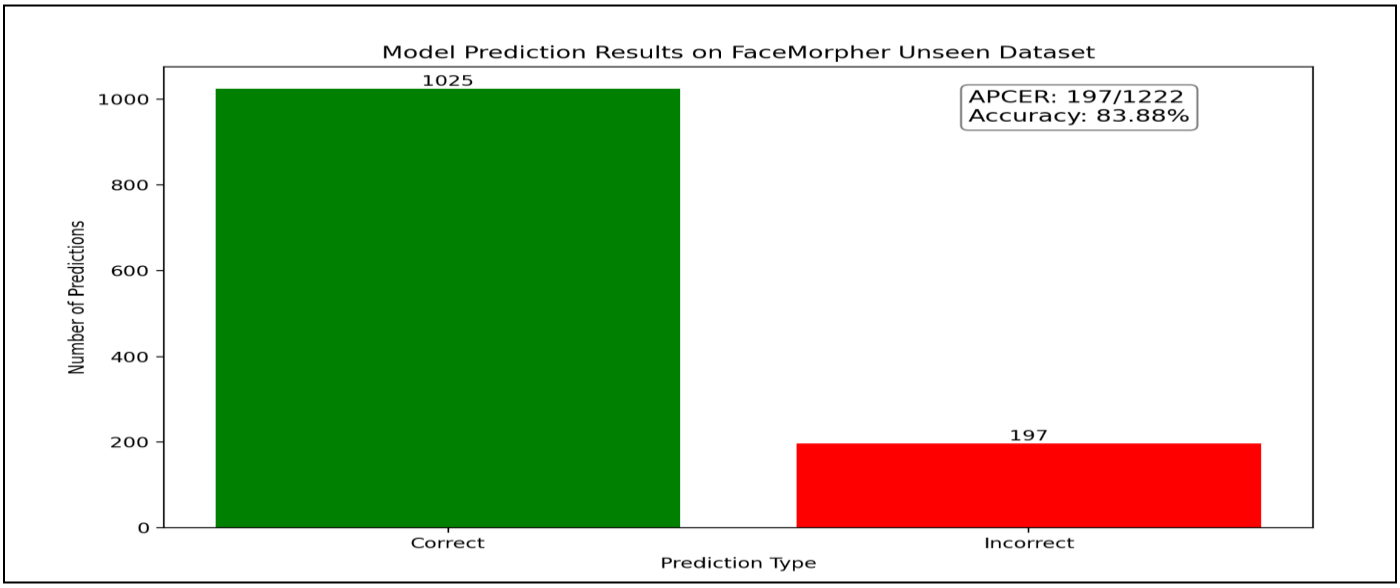

Fig 2 Model Predictions on Unseen Face Morpher dataset

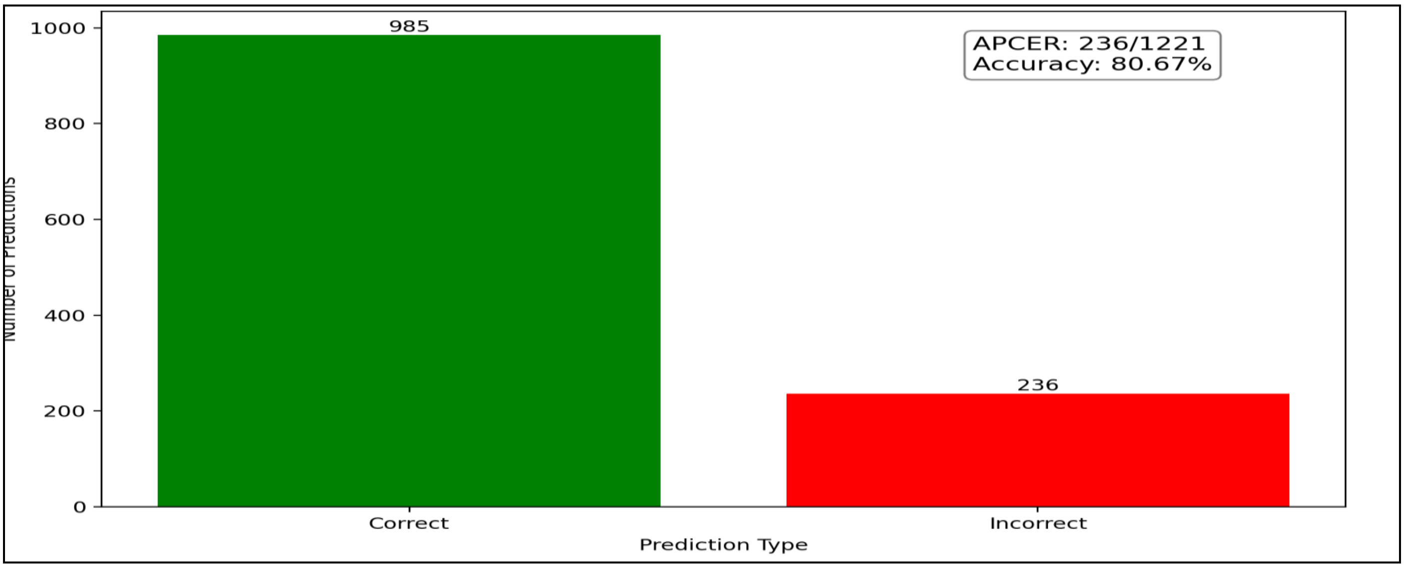

Fig 3 Model Predictions on Unseen Web Morph dataset

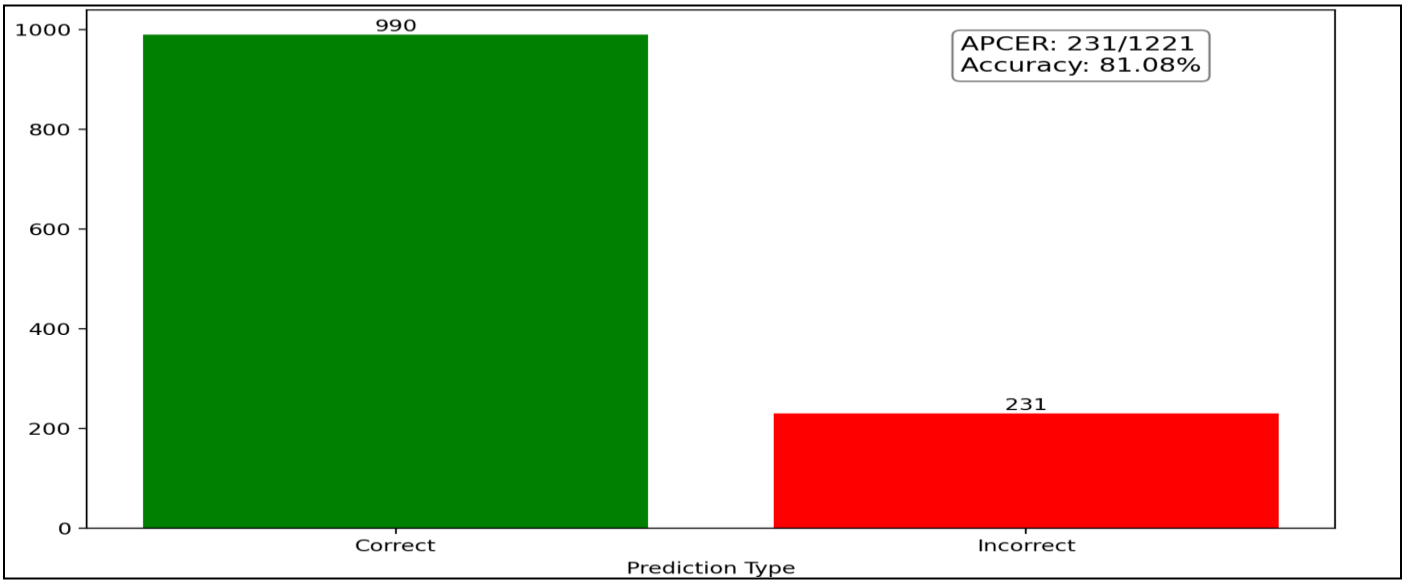

Fig 3 Model Predictions on Unseen StyleGAN dataset

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24AUG1184

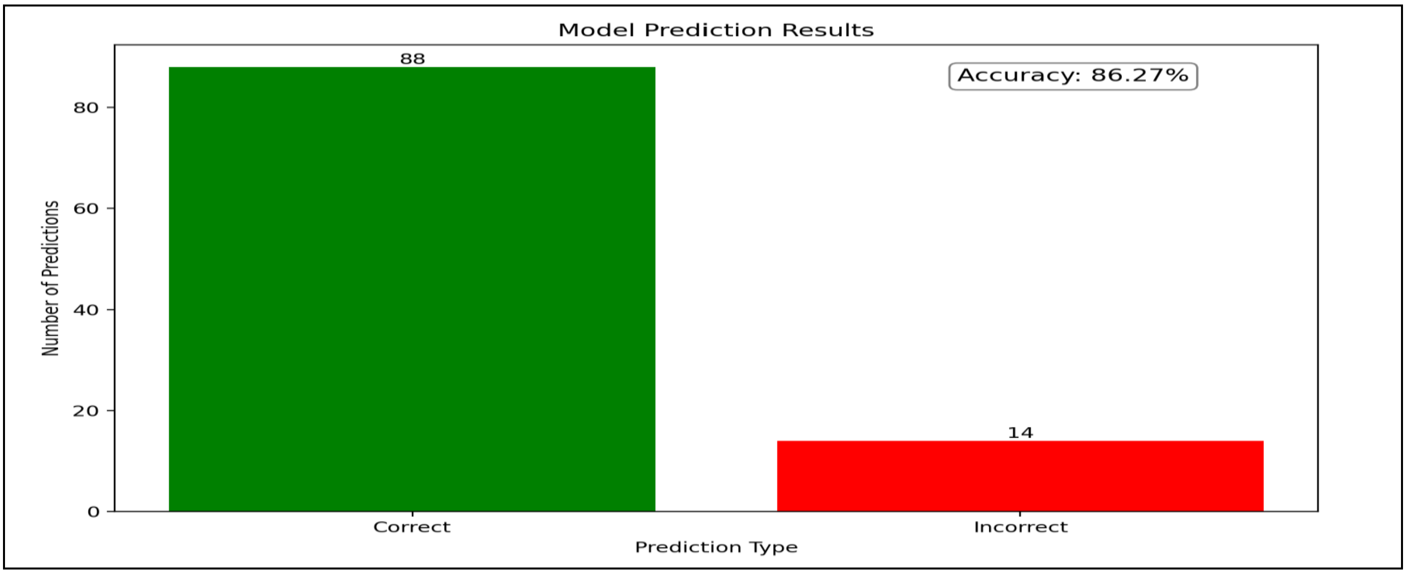

Fig 5 Model Predictions on Unseen Original FRLL Smiling dataset

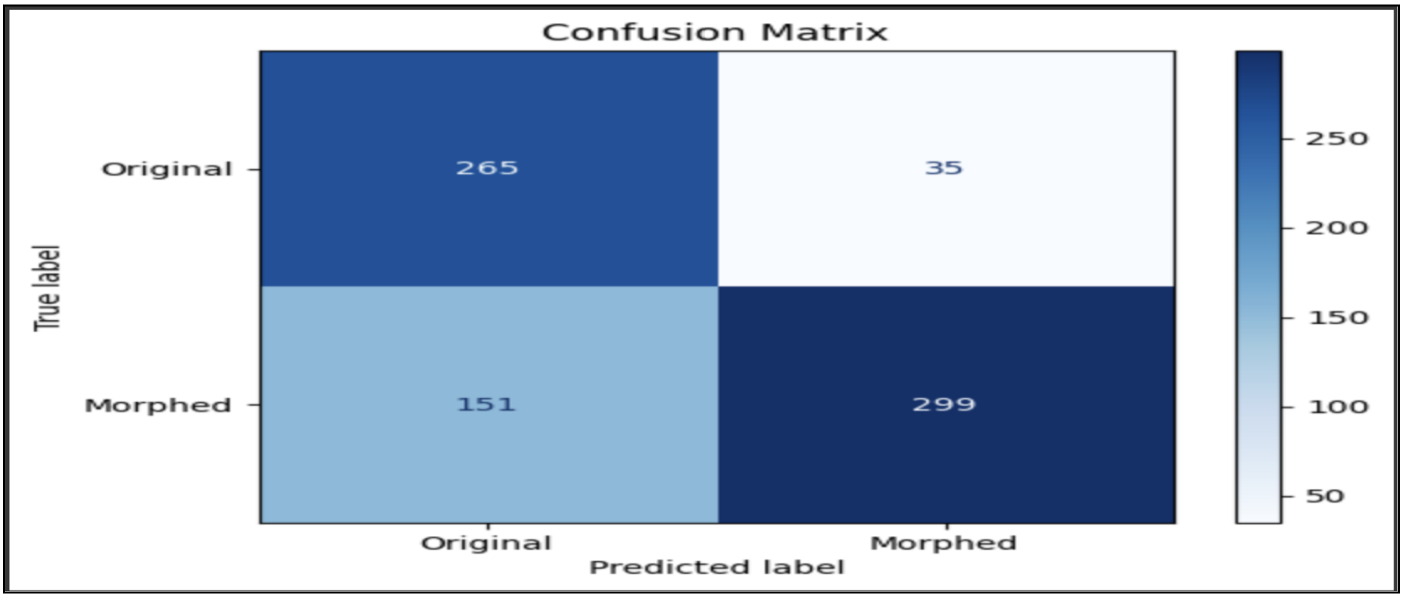

Fig 6 Confusion Matrix of SVM Classifier

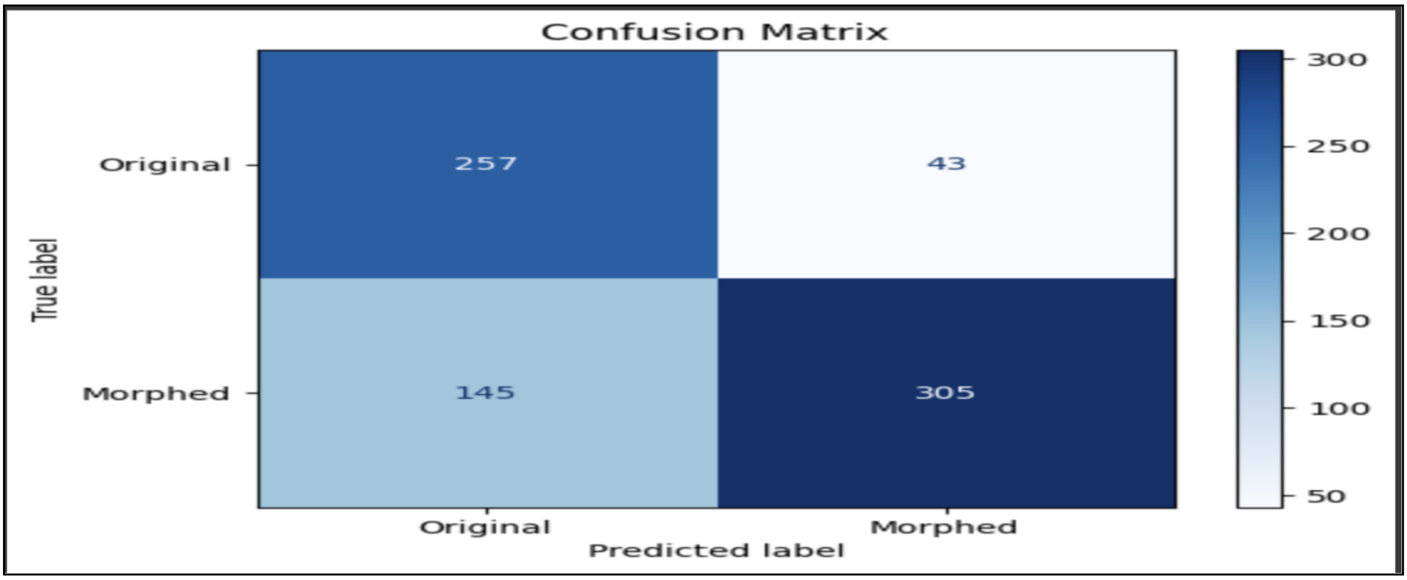

Fig 7 Confusion Matrix of SVM attention classifier

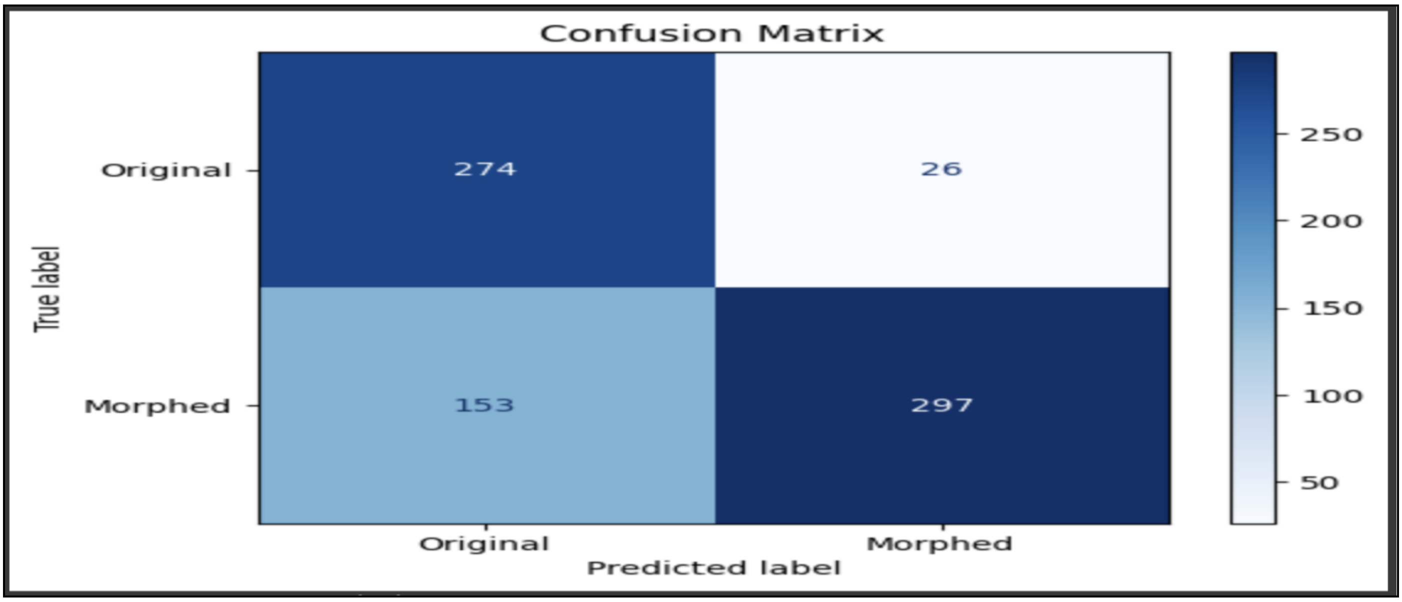

Fig 8 Confusion Matrix of Voting Classifier

VI. RESULTS AND DISCUSSIONS

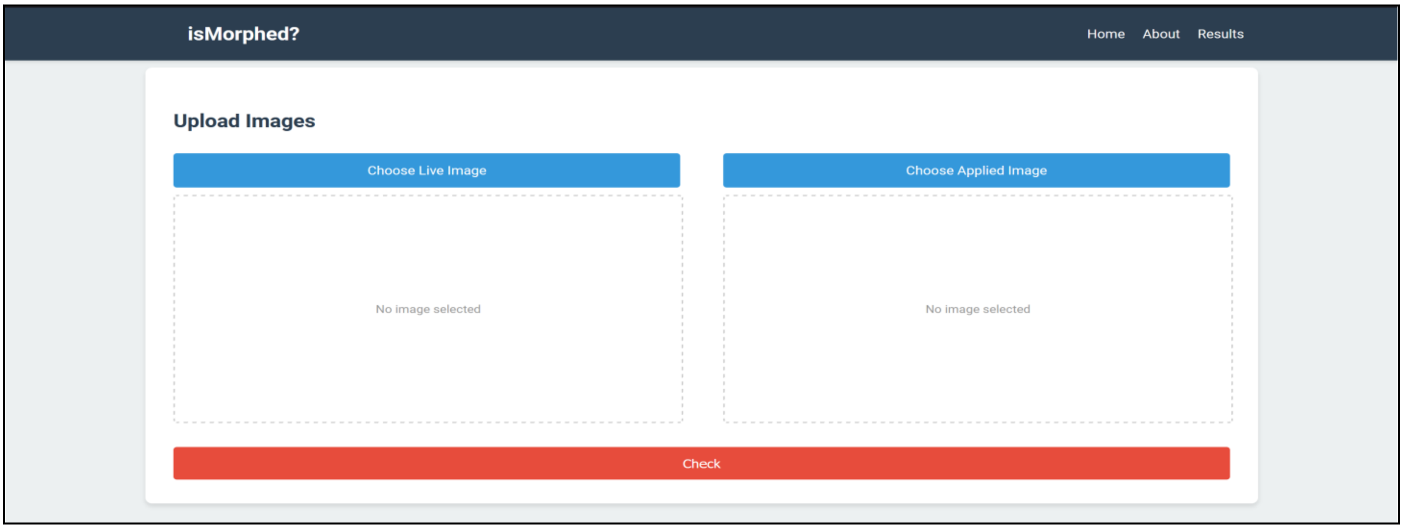

Fig 9 Home Page

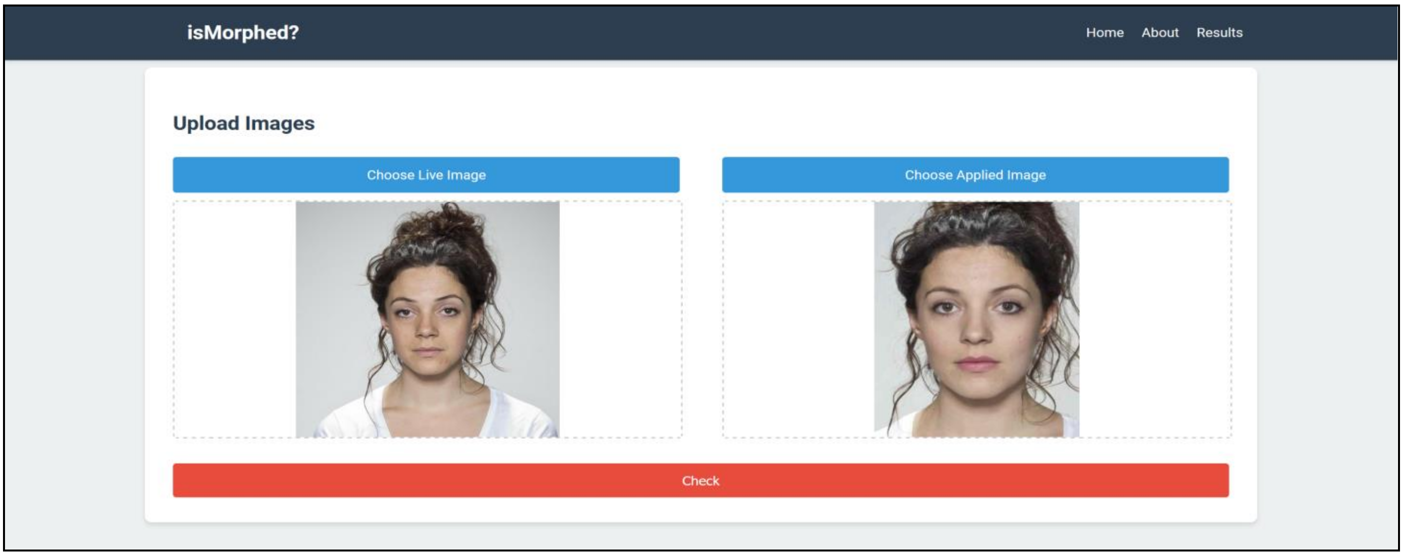

Fig 10 Home Page After user uploading images

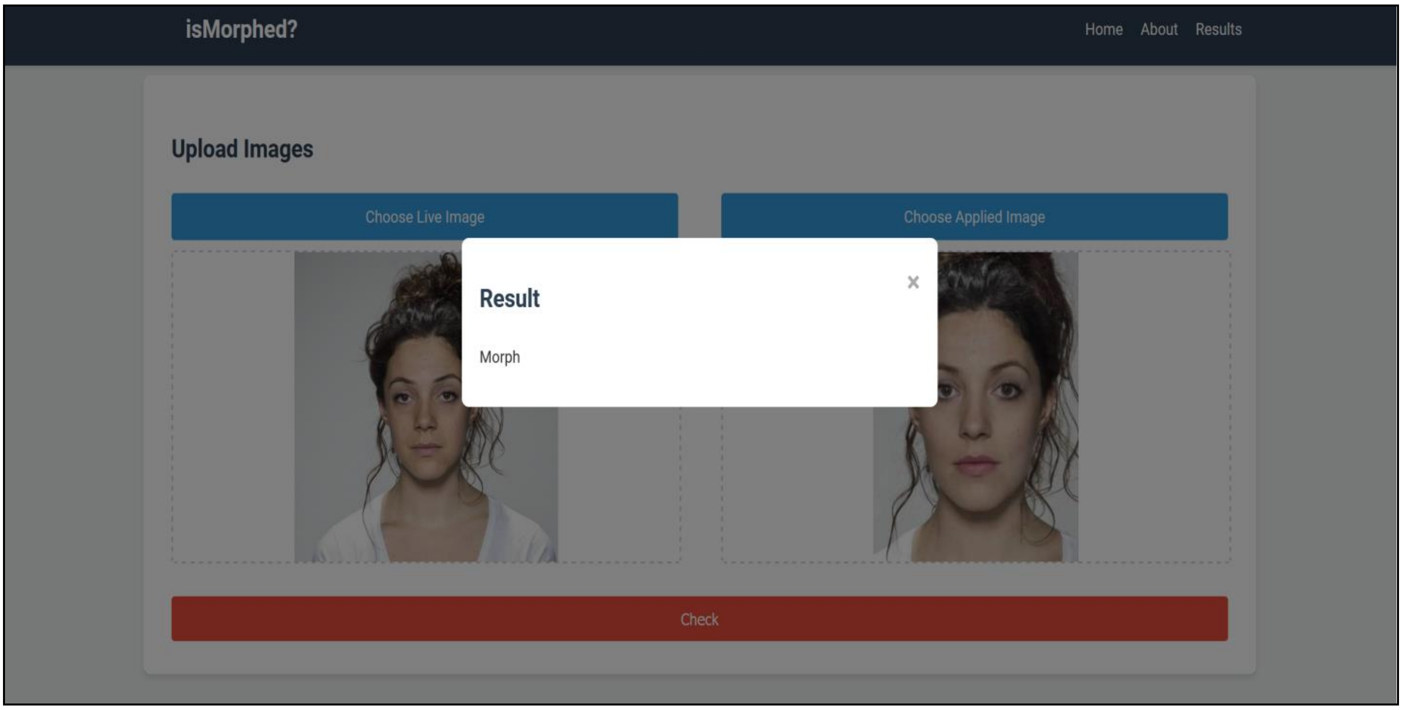

Fig 11 Result was shown in the modal

Here, we got the result as morph because the applicant used a morphed image while applying. However, our system successfully identified it as a morphed image.

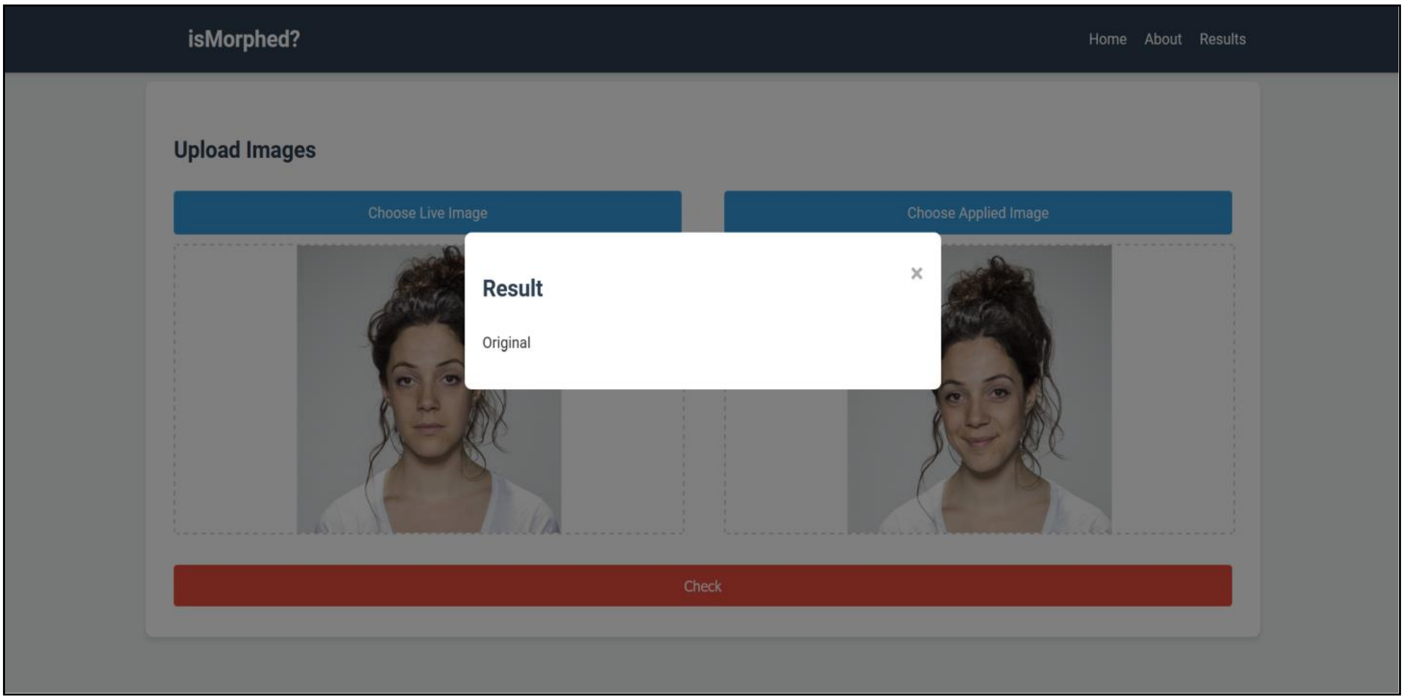

Fig 12 Result was shown in the modal

Here, we got the result as original because the applicant used as an original image while applying. However, our system successfully identified it as an original image.

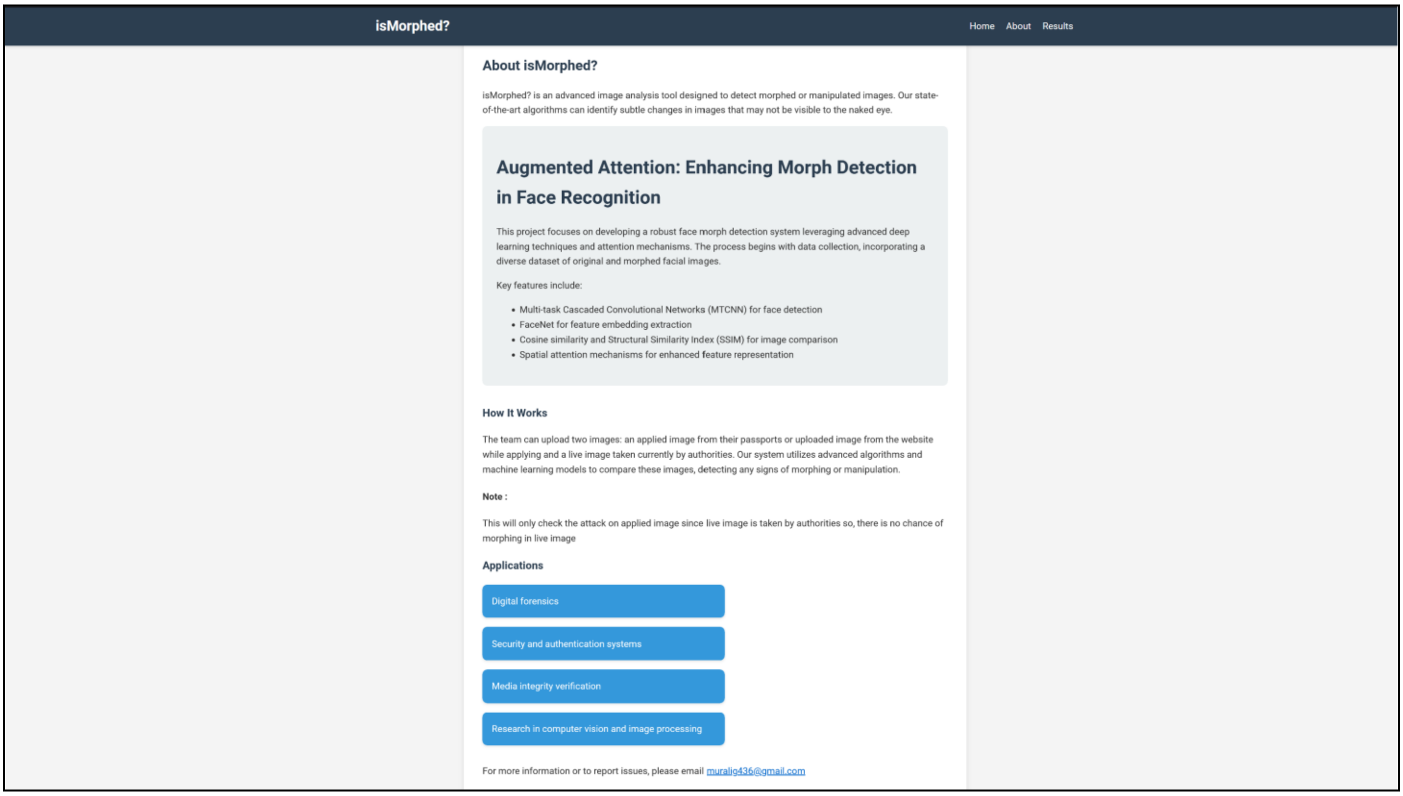

Fig 13 About Page

On the About page, explained the techniques and models used, detailing how our system works and its applications. We've implemented advanced face morphing detection algorithms using deep learning techniques like FaceNet for feature extraction and classifiers such as SVM, Random Forest, and Voting Classifier for accurate detection. The system enhances accuracy by focusing on facial regions and utilizes image similarity measures like SSIM and cosine similarity. Our applications span border control, identity verification, and security systems, aiming to detect and prevent fraudulent activities involving morphed facial images.

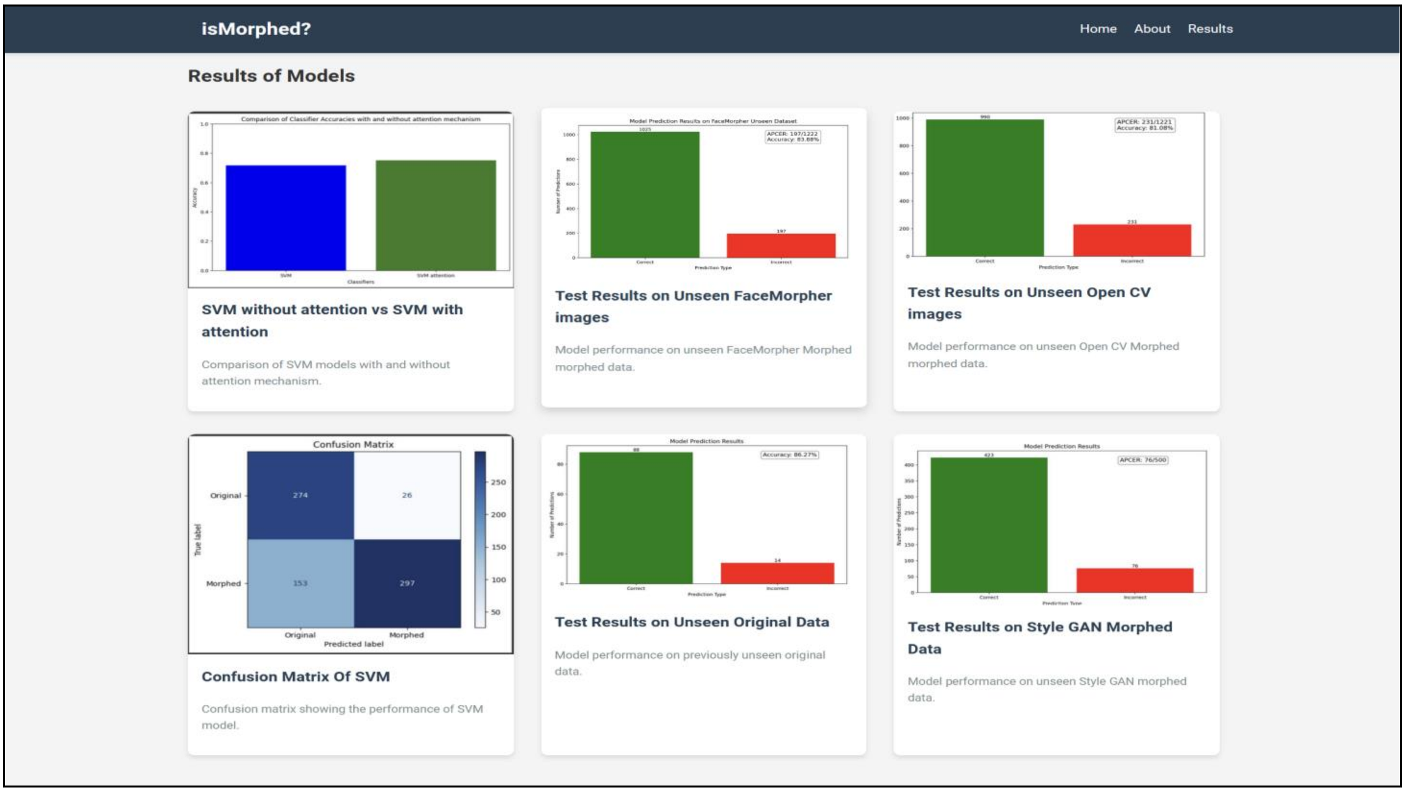

Fig 14 Results Page

In Results Page, we gave a brief introduction on how this model performs on different unseen datasets like you can see in the results page. In this, we compared the performance of SVM model and SVM Model with attention mechanisms as well and analyzed the improvements in accuracies. Confusion matrix will show you the performance of your SVM model, true positives, true negatives false positive and false negative. There are also novelty performance numbers for unseen morphed datasets and original, showing how well the model generalizes to brand new, never seen before images.

VII. CONCLUSION

In this project, we developed a face morphing detection system that accurately classifies images as either morphed or original. We used MTCNN for face extraction and FaceNet for extracting embeddings. We incorporated spatial attention to enhance accuracy and employed a feature combination technique using SSIM and cosine similarity to identify similar images and match original and morphed images effectively. By training machine learning classifiers to differentiate between original and morphed images, we developed a robust system and provided an user-friendly interface ensures accessibility for users from non-technical backgrounds also, making it easy for anyone to use.

FUTURE SCOPE

As technology evolves, new techniques in image morphing will emerge, potentially allowing images to bypass or fool our detection system. Additionally, our current model may struggle to accurately predict images of people from diverse ethnic backgrounds. As future work, we can enhance our model by training it with diverse datasets that include various ethnicities and images morphed using the latest tools and methods. This approach will improve our system's robustness, ensuring it remains competitive and effective regardless of people's backgrounds or the advanced morphing techniques they use, keeping the system up-to-date.

REFERENCES

[1]. Neubert, Tom & Makrushin, Andrey & Hildebrandt, Mario & Kraetzer, Christian & Dittmann, Jana. (2018). Extended StirTrace Benchmarking of Biometric and Forensic Qualities of Morphed Face Images. IET Biometrics. 7. 10.1049/iet-bmt.2017.0147.
[2]. DeBruine, Lisa; Jones, Benedict (2017). Face Research Lab London Set. figshare. Dataset. https://doi.org/ 10.6084/m9.figshare.5047666.v3
[3]. E. Sarkar, P. Korshunov, L. Colbois and S. Marcel, "Are GAN-based morphs threatening face recognition?," ICASSP 2022 - 2022 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Singapore, Singapore, 2022, pp. 2959-2963,doi: 10.1109/ICASSP43922. 2022.9746477.
[4]. Vulnerability Analysis of Face Morphing Attacks from Landmarks and Generative Adversarial Networks. Eklavya Sarkar, Pavel Korshunov, Laurent Colbois, Sébastien Marcel
[5]. ISO/IEC JTC1 SC37 Biometrics, Information Technology-Biometric Pre sentation Attack Detection Part 3: Testing and Reporting, International Organization for Standardization, Geneva, Switzerland, document ISO ISO/IEC IS 30107-3:2017, 2017.
[6]. M. Hamza, S. Tehsin, H. Karamti and N. S. Alghamdi, "Generation and Detection of Face Morphing Attacks," in IEEE Access, vol. 10, pp. 72557-72576,2022,doi:10.1109/ACCESS.2022.3188668.
[7]. Enhanced face morphing attack detection using error-level analysis and efficient selective kernel network, https://doi.org/10.1016/j.cose.2023.103640.
[8]. S. Venkatesh, R. Ramachandra, K. Raja and C. Busch, "Face Morphing Attack Generation and Detection: A Comprehensive Survey," in IEEE Transactions on Technology and Society, vol. 2, no. 3, pp. 128-145, Sept. 2021, doi: 10.1109/TTS.2021.3066254.