EfficientNet B5: A Robust Approach to Detect Morphed Images

Swapnali Ravindra Teli [1], Prof. Prathmesh P. Powar [1]

[1] *M.Tech (CSE) Student, AMGOI, Kolhapur, Maharashtra, India.* swapnaliteli08@gmail.com

[1] *Guide, Assistant Professor, AMGOI, Kolhapur, Maharashtra, India.* pgcse@amgoi.edu.in

Abstract: Data traffic is important in the transmission and exchange of numerous types of data in the digital environment of the global web, including files and photographs. However, this data is susceptible to unauthorized alterations, particularly in the form of morphing, necessitating the development of effective detection mechanisms. The proposed system serves the purpose of identifying morphed images and informing users about their authenticityThe globe Wide Web's digital surroundings witnesses a constant flow of data in the form of files and photos. Unfortunately, data is not immune to tampering, and as a result, it becomes imperative to detect instances of such alterations. The proposed method aims to identify and flag modified photographs, providing users with insights into the authenticity of images they encounterThe academic industry has showed a renewed interest in addressing the subject of morph attack detection in recent years. Various studies and methodologies have been explored to accurately detect instances of morphing attacks and enhance the security of digital content.

Keywords: Convolutional Neural Networks, Event Detection, Morphological transformation, Efficient Net B5.

1. INTRODUCTION

In the age of the technology landscape of the World Wide Web, data traffic plays a significant role in the transmission and exchange of various forms of data, including files and photos. Unfortunately, data is vulnerable to morphing, necessitating the need for effective detection mechanisms. The suggested method focuses on detecting altered photographs and informing users about the validity of the images they encounter. In recent years, the scientific community has made significant efforts to address the problem of recognising morph attacks. Numerous studies and methodologies have been employed in this area to accurately identify instances of morphing attacks and enhance digital content security. While obtaining a sufficient number of morphed images for research purposes can be challenging, researchers often rely on various face databases to create morph image databases. Detecting morphing attacks, especially through facial manipulation, presents a significant challenge. To detect potential morphing threats, automated border control systems use a combination of inspection by humans and automatic classification algorithms. Understanding how machine learning systems can recognise changing faces and focus on crucial facial regions is critical. Texture signal analysis in these crucial areas allows for the differentiation of authentic and altered images, increasing the effectiveness of both automatic and manual inspection methods. This research involves the creation of two types of morphed images:

This research introduces two distinct categories of morphed images:

Morph-3: These images are generated by combining facial images from three different individuals.

Morph-2: These images are created by blending facial images from only two persons.

The objective of this study is to develop a robust and versatile morph attack detection model capable of effectively addressing morphing attacks in real-world scenarios. In recent times, there has been a surge in presentation attacks targeting ID verification systems, emphasizing the need for advanced detection techniques and diverse morphed databases to enhance security measures. For instance, they contrast the user's selfie with an image of themselves taken from their passport or ID card. Verifying if the ID card image has been changed with digitally or physically is a crucial challenge. Picture manipulation is a serious problem for these kinds of situations and biometric systems in general. Numerous unlawful activities can potentially arise from the failure of facial recognition and authentication systems. Present-day facial recognition systems are vulnerable to various biometric attacks. The focus of this

research centers on detecting morphing attacks. This study proposes a dependable detection approach capable of accommodating variances in age, lighting, eye-related changes, and headgear alterations. It employs both a deep learning-based classifier and feature extractor. Additionally, suggestions are made for enhancing images and combining features to enhance detection performance. Notably, this study introduces a novel perspective by examining Morph-3 images, a topic not previously explored in existing literature. Furthermore, it provides a more realistic depiction of morph attack scenarios using professional morphing software.

2. LITERATURE SURVEY

Examining various approaches to combining features, feature concatenation emerged as the most efficient technique for detecting morphed images. Although certain techniques, such as feature concatenation, improved the performance of morph attack detection, there was an associated increase in computing costs. Furthermore, it was observed that models trained on morphed databases with limited variation—generated automatically using low-quality morphing tools like OpenCV and FaceMorpher with the aid of programming scripts—struggled to identify manually created morphed photographs produced using high-quality morphing technologies. The model's performance on test data significantly improved as a result of its training on manually curated morphing databases employing high-quality techniques. In scenarios involving changes in age, lighting conditions, posture, and facial expressions, the proposed strategy produced noticeably good and improved results.

This study proposes a method for automating the retouching of morphing artifacts that uses the Condition Generational Adversarial Network paradigm and Attention Maps to direct the generation process, focussing the retouching on specific regions of concern. The structure is used to handle high-resolution photos in various facial regions. After these regions have been edited and refined, they are smoothly combined to reconstitute the full transformed face.

The sides of the right and opposite eyes, the nostrils, and the roof of the mouth are four separate squared facial parts that are typically affected by artefacts. Various qualitative and quantitative experimental assessments, including pixel-wise measurements, identity preservation, and human observer analysis, have been done to validate the efficiency of this approach.

This study's single based on pictures morphing attack detection (S-MAD) architecture is based on multimodal regions such as the mouth, nose, and eyes. Each of these regions is processed using a colour scale-space representation, from which two types of features, known as local binary aspects (LBP) and transformed statistic image features (BSIF), are retrieved. These features are then fed into classifiers such as the Parametric Collaboration Reconstruction Classification (P-CRC) and the Spectrum The regression The kernel Discriminator (SRKDA). To arrive at a final determination, their decisions are pooled at the score level. Extensive tests are carried out utilising three separate face morphing datasets to evaluate the efficacy of the approach suggested in comparison to existing methodologies.

3. OBJECTIVE

To develop a system that implements Multi-task Cascaded Convolutional Networks (MTCNN) and Efficient Net B5 to detect authenticity of images against morphing.

4. IMPLEMENTATION

There is a lot of data traffic in the digital realm of the realm Wide Web that interprets and transmits data. This data is in form of files, images. Data is prone to morphing and hence detection of such incidents is needed. The proposed system will find out the morphed images and notify the user with images authenticity.

Following are the modules to be implemented in the system.

i. Preprocessing

In this module the dataset of two different images set is feed to the system. The preprocessing step plays a pivotal role in the intricate process of identifying morphed images. This initial phase involves a series of essential operations aimed at enhancing the image data and isolating distinct characteristics that may indicate tampering or morphing. Initially, noise reduction techniques are employed to eliminate any unwanted artifacts or distortions that might obscure

the underlying image structure. Subsequently, image normalization and resizing are applied to ensure uniformity in scale and dimension, facilitating a standardized analysis.

Following this, feature extraction techniques come into play, where essential elements of the image, such as texture, color, and shape, are isolated and quantified. These extracted features serve as critical indicators in discerning potential alterations or inconsistencies within the image. Moreover, various filters and transformations may be applied to accentuate specific details or patterns that could reveal the presence of morphing. The preprocessing step also incorporates error correction mechanisms to rectify any imperfections that may have occurred during the acquisition or transmission of the image data. This ensures that the subsequent analysis is based on accurate and reliable information. In essence, the preprocessing step acts as the foundation for the identification of morphed images, refining the raw image data and extracting pertinent information that is vital for the subsequent stages of analysis and detection.

This dataset are as follows:

1) Morphed Image(Image which we want authenticity of)
2) Related Images to Morphed Images.

Images are being merged into a single dataset based on the relevance. This study involves the generation of two distinct types of morphed images:

Morph-3: These images are generated by blending facial images of three different individuals.

Morph-2: These images are created by merging facial images of only two persons.

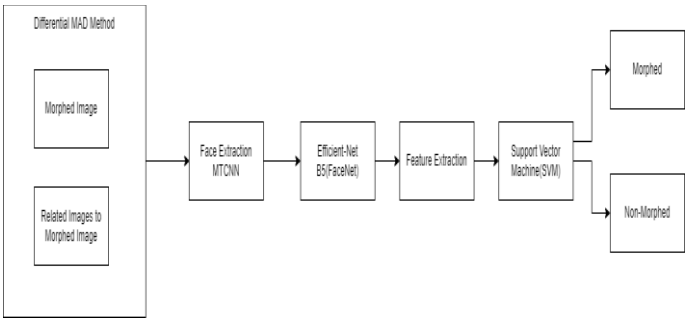

Figure 1. Proposed system

ii. Face Extraction MTCNN

The Multi-task Cascaded Convolutional Networks (MTCNN) is a process that comprises three stages of convolutional networks capable of identifying facial features and landmarks like the eyes, nose, and mouth.

1) Find Boundary of Faces detected.
2) Find facial marks like eyes ,Nose,lips etc.
3) Convert Extracted Image to fix size.

Following are the three tasks of the MTCNN that are face/non-face classification, bounding box regression, and facial landmark localization.

iii. Efficient Net B5 and Feature extraction

EfficientNet is a convolutional model (ConvNet) that offers a novel scaling method for uniformly adjusting depth, width, and resolution dimensions using a straightforward yet highly efficient compound coefficient. It is employed to extract features from input images in combination with FaceNet. The system captures input features live and combines them with potential morph images through operations like subtraction, addition, or concatenation. After verification, these combined features from a potential morph and its corresponding live-captured image contribute to the development of a facial recognition system.EfficientNet B5, recognized for its exceptional efficiency and accuracy, serves as the architecture of choice for feature extraction in the context of morphological image detection. When applied to this

domain, EfficientNet B5 serves as a robust backbone network, capable of automatically discerning intricate patterns and structural nuances within images that are crucial for identifying morphological variations. The feature extraction process entails leveraging the hierarchical layers of the EfficientNet B5 model to capture both low-level and high-level features within the images. In the initial layers, it identifies basic elements like edges, colors, and textures, while the deeper layers progressively assemble these elements into more complex and abstract features, ultimately encapsulating the unique morphological characteristics of the images. This extracted feature set, often referred to as the network's embedding, is a representation of the images that retains their morphological information in a condensed and meaningful form. These embedding serve as a foundation for subsequent classification or detection tasks. The EfficientNet B5 architecture's exceptional depth and parameter efficiency ensure that these features are both comprehensive and discriminative, enabling accurate morphology detection with reduced computational complexity. In summary, EfficientNet B5 excels as a feature extraction tool in morphology detection, harnessing its deep learning capabilities to automatically uncover and encode essential image attributes. Its ability to efficiently distill the rich morphological information within images makes it a valuable asset in the realm of image analysis and pattern recognition for various applications, including medical diagnostics and quality control in manufacturing.

iv. SVM classifier Technique.

The combined features undergo analysis by a machine learning-based classifier known as SVM (support vector machine) to make a determination regarding whether the input images are morphed or genuine. This assessment involves calculating both the cosine distance and SSIM score between the potential morph and the corresponding live-captured images. Cosine distance quantifies the similarity score using feature vectors extracted from the input images, while SSIM evaluates the similarity score using the extracted face images. To integrate these scores, an averaging technique is applied. The final decision hinges on the lowest combined similarity score between cosine distance and SSIM, ultimately leading to the fusion of features from the potential morphed image with those from the live-captured image.

v. Evaluation and classification.

In this final module a prediction is being passed based on the evaluated images and a output is passed if the images are morphed or not. Following the feature extraction process, the next crucial step in image morphology detection involves evaluation and classification, often performed using the Support Vector Machine (SVM) classifier technique. SVM is a powerful machine learning algorithm that excels at distinguishing between different classes based on the extracted features. In this stage, the SVM classifier utilizes the feature set generated by methods like EfficientNet B5 to make informed decisions about the morphology of the images. The classifier is trained on a labeled dataset, learning the underlying patterns and relationships between features and specific morphological characteristics. This training phase is essential for the SVM to generalize its knowledge and accurately classify unseen images. Once trained, the SVM classifier is put to the test, assessing its ability to classify images into predefined categories or classes, each representing a distinct morphological attribute. The classifier computes a decision boundary or hyperplane in the feature space, aiming to maximize the margin between different classes while minimizing classification errors. The effectiveness of the SVM classifier is measured through various evaluation metrics, such as accuracy, precision, recall, and F1-score. These metrics provide insights into the classifier's performance, shedding light on its ability to correctly classify images based on their morphology. Additionally, techniques like cross-validation are often employed to ensure the model's robustness and prevent over-fitting. In conclusion, the integration of the SVM classifier technique into the image morphology detection pipeline is crucial for making sense of the extracted features and assigning images to their respective morphological categories. Through rigorous evaluation and classification, this approach enables the automation of morphology detection tasks, offering enhanced accuracy and efficiency in fields like medical imaging, quality control, and beyond.

vi. Result and Analysis

Accuracy:

Accuracy is a fundamental and critical parameter when evaluating the performance of image morphology detection systems. In the context of these systems, accuracy measures how effectively the model can correctly classify images as either morphed or genuine. It serves as the primary metric for assessing the system's overall effectiveness and reliability. A high accuracy rate indicates that the system excels in distinguishing between morphed and authentic

images, minimizing false positives and false negatives. In practical terms, a high accuracy score means that the system is successful in identifying potential instances of image manipulation, providing confidence in its ability to protect against morphing attacks. However, in order to acquire a more full view of the system's performance, accuracy must be considered with other measures like as precision, recall, and F1-score. Precision is the percentage of actual positive categorization out of every one of the favourable projections, whereas recall is the percentage of actual positives based of all real positive cases. The F1-score combines precision and recall to provide a balanced assessment of the model's abilities. The correct mix of precision, reliability, and recall is critical in picture morphology recognition. A system with excellent resolution however low precision may produce a large number of false positives, resulting in unnecessary alarms. A high-recall system, on the other hand, may miss certain modified photos, jeopardising security. Therefore, achieving a harmonious blend of these metrics is essential for building a robust and dependable image morphology detection system. In conclusion, accuracy plays a central role in evaluating image morphology detection systems, reflecting their ability to correctly identify morphed images. While accuracy is a pivotal parameter, it should be considered alongside other metrics to ensure a comprehensive assessment of a system's performance and its suitability for specific applications, ranging from security to quality control.

5. CONCLUSION

Pre-processing is the module that mainly focuses on the image gathering which are basically once that is morphed and others that may be possible match to the morphed one. In this module we obtain a set of images that will be bunch of all the images that can help us identify the morphed image. The face extraction module gives us results of different faces detected based on the MTCNN algorithm. Hence the system implemented has\given us the desired results with excellent output. In today's digital realm, where data traverses the vast landscape of the World Wide Web, safeguarding the integrity of information is paramount. The exchange of data in various forms, including files and images, is ubiquitous, but it's also susceptible to manipulation and morphing. This challenge underscores the need for robust systems capable of detecting morphed images and ensuring the authenticity of visual content. In response, this paper presents a comprehensive approach to address this issue.

The research community has been increasingly focused on the critical problem of morph attack detection, leading to various innovative methods. These efforts have been instrumental in advancing our ability to identify morphed images and protect against the misuse of digital information. Importantly, this study introduces a diverse morphed image database, including both Morph-2 and Morph-3 images, enhancing the practicality of morph attack detection scenarios. The proposed system encompasses several key modules, beginning with preprocessing. This foundational step involves noise reduction, image normalization, and feature extraction, which collectively refine the raw image data and extract essential characteristics for subsequent analysis. Leveraging state of art techniques like Efficient Net B5, the system excels in feature extraction, capturing intricate patterns and structural nuances and Efficient Net B5 renowned for its efficiency and accuracy, serves as a potent tool for morphology detection. It extracts a rich feature set from images, enabling the system to discriminate between morphed and genuine content effectively. Furthermore, the SVM classifier technique, a powerful machine learning tool, is employed to classify images based on their morphological attributes. The classifier is trained to recognize patterns and relationships within the feature space, ensuring accurate categorization of images. The system's evaluation and classification phase are critical for assessing its performance. Metrics like accuracy, precision, recall, and F1-score provide valuable insights into the classifier's effectiveness. Cross-validation techniques enhance the model's robustness and prevent overfitting, ensuring reliable results. In conclusion, this paper presents a holistic approach to tackle the challenge of morph attack detection in digital images. By combining preprocessing, feature extraction with EfficientNet B5, and SVM classification, this system offers a comprehensive solution to identify morphed images accurately. In an era where data integrity is paramount, such systems play a pivotal role in safeguarding the authenticity of digital content, with applications spanning from security to quality control in various industries.

6. REFERENCES

[1] Alva Erwin, Raj P. Gopalan, N.R.Achuthan,“ Efficient Miningof High Utility Item set From Large Data set” Nov 2015

[2] C.F.Ahmed, S Khairuzzaman Tanbeer,Byeong-Soo Jeong, Young-Koo Lee,” Efficient Tree Structure for High Utility Pattern Mining in Incremental Databases”Nov 2015

[3] Menghchi Liu, Junfeng Qu,” Mining High Utility Item set Without Candidate Generation”, Nov 2015.

[4] Vincent S Tseng, Bai-En Shie, Cheng Wu, Philip SYu,“ Efficient Algorithm For Mining High Utility Item set from Transactional Databases”, Nov 2015
[5] Yao H and Hamilton Hj “ Mining item set Utility from Transaction database” Nov 2015
[6] Yung Liu, Woe heng Liao and Alok Choudhary,” A Two Phase algorithm for Fast Discovery of High Utility Item set” Nov 2015
[7] H.F.Li, H.Y.Hung, Y.C.Chen, Y.J.Liu and S.Y. Lee” Fast and Memory Efficient Mining Of High Utility Item set in Data Stream” Aug 2015
[8] Mahdi Esmaeili and Fazekas Gabor,” Finding Sequential Pattern from Large Sequence” May 2015.
[9] D. G. Lowe, “Object recognition from local scale-invariant features,” in Proc. 7th IEEE Int. Conf. Comput. Vis., vol. 2. Sep. 1999, pp. 1150–1157.
[10] Q. Mei, C. Liu, H. Su, and C. Zhai, “A probabilistic approach to spatiotemporal theme pattern mining on weblogs,” in Proc. 15th Int. Conf. World Wide Web, 2006, pp.533–542.

DOI: https://doi.org/10.15379/ijmst.v10i4.2379