International Journal of Biomedical Research & Health Sciences

IJBRHS | Volume 2 Issue 1

Face Morphing Attack Detection-A Literature Review

Gourav Rawat [1*], Harshita Gupta [2], Shah Faisal [1], Mohammad Hashir [1]

[1]Department of Computer Science and Engineering, School of Engineering and Technology, Sharda University, Greater Noida, India

[2]Department of pharmacy, School of medical and allied Sciences, G.D. Goenka University, Sohna road, Gurugram

[*]**Corresponding author**: Gourav Rawat, Department of Computer Science and Engineering, School of Engineering and Technology, Sharda University, Greater Noida, India Email: rgourav174@gmail.com

Received date: 25-Feb 2024, **Accepted Date:** 12-Mar-2024, **Manuscript No.** ijbrhs-23-0006, **Published date:** 20-Mar-2024

Abstract

Face morphing is a sophisticated kind of image manipulation that involves combining two or more facial photographs to create a new identity. This technique is becoming more and more common in digital media, and it might lead to major issues including fraud, identity theft, and the propagation of bogus identities. The goal of this study is to solve these problems by developing a face-morphing detection system that uses state-of-the-art computer vision and machine learning techniques to be both accurate and efficient. To identify morphed faces, the proposed method examines minuscule aberrations and inconsistencies created during the morphing process. It accomplishes this by applying feature extraction methods and deep neural networks. By evaluating the system's resilience on a large dataset that encompasses several morphing techniques and lighting configurations, its effectiveness is confirmed in a multitude of scenarios.

Keywords: Face Morphing attack, Biometrics, Morphed image, MADs, SVM

Introduction

High- Biometrics is a method of identifying people according to their distinctive traits. Facial recognition is a widely used biometric technique [1]. These days, biometric verification technologies are extensively used for both commercial and state purposes, such as border control. Lately, reliable, and accurate neural networks for the detection of face-morphing attacks [2]. To improve resilience and generality in safety and security-related applications, particularly for face morphing attack detection, the research proposes neural network training strategies [3]. Developing a training technique to strengthen neural networks' defenses against assaults on their ability to make decisions and applying it to the training of a better face-morphing attack detector. Tolerance for intra-subject variances is exploited by morphing attacks, and morphed pictures can be used to trick FRS systems. An automated border control system is in place for authorization and authentication [4]. In facial recognition systems, fraudulent operations also employ face morphing. Ina larger sense, there are two distinct types of morphing attacks: (i) using digital pictures for morphing assaults and (ii) utilizing re-digitized pictures for morphing assaults [5]. Understanding themorphing process and its final traces is crucial for preventing morphing attacks. Morphing detection should be integrated at both the application stage for new documents and the identity verification step of document consumption.

Three indicators may be used to identify morphed photographs. Suspicious resemblance to other gallery images, visual artifacts of blending caused by imperfect superimposition of face components, and inherent content- independent signs of image alteration [6]. Intentional anti-forensic picture alterations may impede the detection of inherent morphing Traces. Most of the earlier research employed training and testing data using the same pairing criterion, which often selects faces that are similar, without considering generalization issues or potential benefits from actual modifications to such a methodology. The impact of employing various morph pairing techniques has been investigated recently. Among other things, this work highlighted the importance of training data pairing for overall detection performance [9]. Perception by humans: Morphing assaults are designed to fool human observers, such as border guards and ID specialists. According to studies, it is difficult for human observers to identify modified facial photos, therefore relying just on human judgment for detection is problematic. Absence of training data: Previous research on the interpretation of morphing pictures by humans relied on untrained student observers and only offered one image for analysis, which might not be a reliable representation of real-world situations. The absence of extensive and varied training data impedes the creation of efficient detection systems. [7] Accessibility of morphing tools: A wide range of openly accessible tools make it simple to create morphed face photos, boosting the technique's use and potential for abuse. The fact that these technologies are widely accessible makes it difficult to identify morphing assaults with accuracy. sophisticated morphing methods: As morphing methods have developed; it is now challenging to identify changed facial photos. To accurately detect minor morphing artifacts and separate them from real facial characteristics, deep learning techniques and advanced algorithms are needed. Benchmarking and evaluation:Standardized datasets and performance criteria are needed for the assessment and benchmarking of morph attack detection (MAD) algorithms. A thorough and varied database infrastructure is essential for assessing and comparing MAD algorithms, as well as for reliable evaluation and comparisonof various detection methods. risks that are always changing: As technology develops, new attack tactics and morphing techniques might appear. To stay ahead of these risks, effective detection systems must be continuously researched and developed [8].

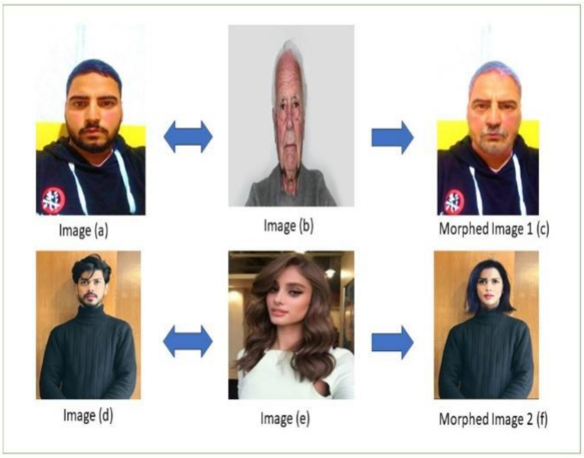

Fig. 1. Morphed image

The goal of face morphing attacks is to fool facial recognition systems (FRSs) into granting illegal access by creating a morphed face picture. Algorithms for detecting and averting morphological assaults (MADs) are created. Deep learning methods, differential image-based analysis, texture-based analysis, and other techniques are employed by MAD algorithms. Metrics like as false rejection rate (FNMR) and benchmarking tests like the FRVT MORPH test are used to assess the performance of MAD algorithms. facial morphing assaults are a challenge to creating a safe society, despite the growing faith in facial recognition systems (FRSs) for security- related applications.

Numerous methods for detecting morphing attacks have been suggested, such as deep learning techniques, differential image-based analysis, and texture-based analysis. However, the development of high-quality morphs because of advances in deep learning and machine learning approaches makes it difficult to generalize morph attack detection algorithms. A fundamental difficulty is still obtaining huge public datasets with variants and diverse morph creation approaches. Metrics like as the Actual MMPMR (AMPMR) can be used to quantify the degree of susceptibility that FRSs must altered pictures. A persistent problem in the discipline is the development of reliable methods for morph detection, which may be used as a guide for future research.

The applicant provides the facial image in digital or analog form for usage in the ePassport application procedure in several countries. In the event of a face-morphing attack, a wanted person may combine the features of a lookalike accomplice with their own. The accomplice will obtain a legitimate passport with matching document security features if he applies for one using the modified face image. It is significant to remember that altered face pictures have the potential to deceive commercial face recognition systems and human examiners by seeming realistic enough. Then, it would be possible to effectively compare the criminal and the accomplice with the altered image that was kept in the ePassport.

Not only is the texture altered throughout the morphing process, but the image's whole signal is also altered. Thus, an additional method of identification might involve examining variations in the sensor noise pattern, such as PRNU. Hence, from a face picture, the PRNU pattern which results from flaws in the camera's sensor and varies for every model as well as every single camera extracted, and the discrete Fourier variables are computed. The resulting histogram is then used to calculate the mean value and variance. A revised version of this approach, based on PRNU variance analysis across picture blocks, was recently suggested by Debias et al. Zhang et al.'s comparable strategy has been put out, demonstrating the value of morph identification based on sensor.

Continuous picture degradation-based morphing attack detection techniques were presented in. These approaches' main concept is to repeatedly degrade the picture quality for example, by compressing a JPEG file n order to produce several fake self- references of a face image. Then, morph identification is performed by analyzing the distances between these references and the original picture. According to Ramachandra et al, high- frequency analysis is advised. Using their method, photos are transformed into grayscale, a controlled pyramid is constructed, and high-frequency training is done on a Collaborative Representation Classifier (CRC).

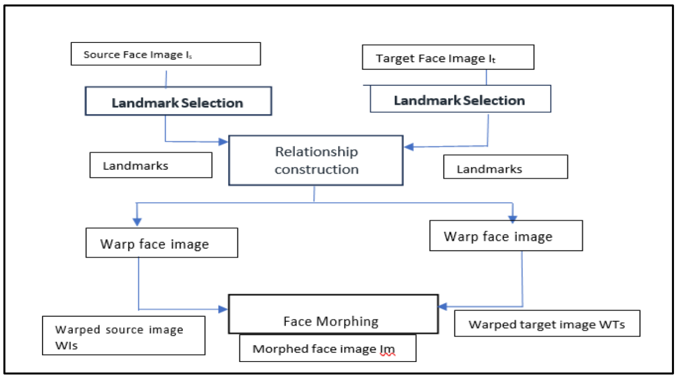

Fig. 2 Overall flow of Face Morphing Attack.

2. Literature Review

In the literature, face morphing has been thoroughly examined, with particular attention paid to full-face and partial- face morphing methods. It has been discovered that partial morphing of areas, including the nose and eye, presents a serious risk to commercial facial recognition systems (FRSs). [9] Although quality-based methods have been developed to identify altered photos and study image deterioration, their effectiveness is restricted to print-scan data. Face De-morphing methods have been proposed to disclose the component pictures utilized in morphed photographs, including deep CNNs and landmark-based morph creation. However, in real-life scenarios with changes in illumination and posture, their performance deteriorates.

Recent years have seen a large amount of research on morphing assaults in biometric systems, leading to advancements in automated generation and visual quality. Often used programs for combining photos in morphing attacks include the GIMP Animation Package (GAP) and the GNU Image Manipulation Program (GIMP). Several morphing strategies have been used to enhance the results of morphing assaults, including the Delaunay-Voronoi triangulation algorithm (DVT) and swapping strategies.[10] Morphing assaults have been identified using spectrum analysis using the Fourier transform, micro-texture analysis, and spatial descriptor occurrences. Using corpora like VGG19, Alex Net, GAN, Face Net, and VGG-Face, convolutional neural networks (CNNs) have been effectively used to identify morphing assaults.

High-quality performance is offered by commercial morphing software, but researchers sometimes have to manually alter and create a enough number of photos for their studies.

De-morphing is the process of dissecting the chip picture and distinguishing between non-morphing and morphed images. The reproducibility of results is hampered by the fact that most published methods were trained and tested on private databases. Large datasets of real and transformed facial photos are not yet available to the public, which makes thorough experimental assessments challenging.

For morph identification, general-purpose image descriptors such as Binarized Statistical Image Features (BSIF) and Local Binary Patterns (LBP) have been proposed.[11]

Many image descriptors have been combined and assessed for morph identification, including LBP, BSIF, SIFT, SURF, HOG, and deep face features.

The Fourier Spectrum of the PRNU is analyzed using PRNU- based morph detection techniques, which measure the spectral variations between morphed and authentic pictures.

Attacks using face morphing entail taking many faces and averaging or mixing them together to create a composite image that looks like a real person. This composite picture is used in a variety of fraudulent operations to mimic real people.

TABLE 1. A Systematic Review of Literature Survey

Paper	Methodology used	Data Set	Performance	Gap Analysis
[1] (2023)	- Extracting embeddings using deep learning-based FRSs - A pair-selection module for morph pair pre-selection based on similarity	- There were 22,992 samples from 3,337 participants in the data set. Using this data set, the vulnerability of several facial recognition systems was investigated.	NA	How well different morphing algorithms mislead FRSs is measured. . insufficient study of pre-selection using various FRS embeddings.

[2] (2021)	Methods for general image quality assessment (IQA) - Face image quality (utility) evaluation techniques (FIQA)	The study's dataset comprises 276 digital morphing assaults (D-M) and 364 digital bona fide (D-BF) photos. Digitized pictures of assaults (PS-M) and bona fide (PS-BF) are also included in the collection.	- Differences between morph and bona fide photos are displayed by Mag Face and SER-FIQ. - MEON records degradation in picture quality in the nose and ocular areas.	- Examining how face morphing affects image quality and usefulness: There isn't a direct link between morphing artifacts and image quality measurements.
[3] (2020)	The study of decision-making processes using neural network training techniques based on training data alternations and Layer-wise relevance propagation (LRP).	The original and modified face photos make up the dataset. Eighty percent of the original photographs are in the training set.	- A variety of training techniques were examined and suggested. In terms of robustness, the suggested multiclass pre-training performed better.	- In order to improve face morphing assault detection's resilience and generality, the study suggests neural network training approaches. The study contrasts two more face-morphing assault detectors with the neural network-based detectors.

[4] (2017)	- Three distinct deep convolutional network topologies are analyzed, and a completely automated morphing mechanism is developed.	- Four disjunctive sets are created from the data set. Both original and altered photos are included in the data collection.	- The FRR of VGG19 (pretrained) is lower than Alex Net (pretrained) and Goog LeNet (pretrained). - All network architectures performed better with pretrained networks.	The small size and privacy concerns with the current face databases
[5] (2019)	- Texture descriptors - Forensic image analysis	Splitting face databases is necessary for both evaluation and training. It is important to disclose the quantity of samples and comparisons made.	- Detection performances achieved are promising and highly robust. - MAD approaches should be transparent and based on sufficient data.	- There are no standardized measures available for assessing MAD procedures. - Evaluation procedures haveto be open and grounded in enough information.
[6] (2019)	- For face identification, VGG and Face Net neural networks - SVM classifier with visual quality measures for detection	- Deepfake video collection made accessible to the public; produced on the Vid TIMIT database using a GAN-based method	- Face recognition systems vulnerable to deep morph videos - Visual quality metrics lead to best performance	- Vulnerability of face recognition to deep morph videos - Need for automated methods to detect GAN-generated faces
[7] (2020)	- The face verification system's morphing detection module is used in the morphing process to produce realistic pictures.	- Training data set: FRAV-ABC-Train with 1000 subjects - Test data set: FRAV-ABC-Test with 170 subjects	- In comparison to literature values, the de-morphing design obtained an extremely low equal error rate (EER). The results support a reliable approach with excellent accuracy levels.	NA
[8] (2022)	Self-morphs are formed by applying face morphing to photos of the same identity and are used in the approach. Borghi et al. first proposed this idea, which is utilized to produce photographs with observable artifacts.	A large-scale face recognition dataset, VGGFace2 has 360 samples per class, 9,000 classes, and 3 million photos. The reason the authors selected this dataset is that, crucial to their filtering approach, each identity has a high average number of samples.	The system produced equivalent results in various protocols and outperformed previous strategies in challenging manual morphs and identifying landmark-based morphs. In comparison to alternative methods, it also demonstrated consistent performance across all protocols.	The limitations of the present stage, such as not taking into account digitalized face photos and using landmark-based approaches for face morphing, are some of the future research objectives that are stated in the report. The authors also state that they want to investigate GAN-based techniques and modify the approach for the differential case.

Examine many ways for morphing images to blend numerous faces, including feature point-based, optical flow-based, and Delaunay triangulation-based techniques. Gaining knowledge about the technical components of these methods might help identify possible weaknesses and detection approaches.

Methods of detection: Examine several techniques, such as deep learning-based techniques, frequency domain analysis, and picture quality analysis, for identifying face morphing assaults. Analyze each approach's advantages and disadvantages as well as how well it works in various situations.

Biometric system vulnerabilities: Examine how face morphing assaults affect biometric systems, including face recognition and authentication. Examine potential countermeasures and evaluate the dangers and difficulties that might arise from using biometric data in security applications. Implications for security and privacy: Examine the moral and legal ramifications of face-morphing assaults in relation to data security and privacy. Think about the possible repercussions of someone misusing a person's biometric data or gaining illegal access to confidential information. Strategies for preventive and countermeasures: Investigate the creation of strong defenses and preventative tactics to lessen the dangers of face-morphing assaults. Analyze these tactics' performance in practical settings and their suitability for incorporation into current security frameworks.

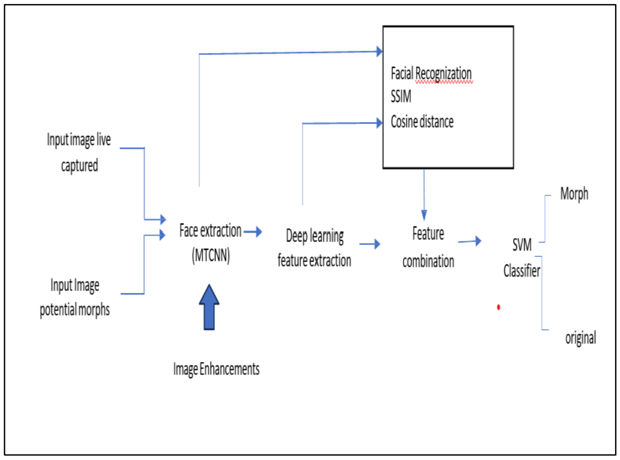

Fig. 3 Morphed Attack Detection Model Design

3. Limitations

Complex Morphing procedures: Face morphing technologies have gotten more complex, making it difficult to identify altered photographs with straightforward procedures. Sophisticated morphing methods can provide smooth transitions between two faces, making it challenging for conventional detection algorithms to distinguish between the morphed regions. Adversarial Attack Evolution: Adversarial assaults have changed throughout time to evade detection measures that are currently in place. Expert attackers possess the ability to edit or create photos that can fool even the most sophisticated face-morphing detection technologies. [19] To combat these constantly changing dangers, detection techniques must be updated and improved on a regular basis. Data Scarcity: The creation of efficient detection models may be hampered by the lack of large datasets with altered pictures. It is difficult to teach machine learning algorithms to detect and differentiate morphed photos from real ones without a large collection of morphed faces.

Computational Complexity: Real-time face morphing detection can have a high computational complexity. It takes alot of processing effort to identify altered faces in a big dataset or in real-time applications, which isn't always possible or useful for many systems.[20] Problems with Generalization: Face morphing detection models may find it difficult to adapt to novel morphing strategies that were not used in training. Consequently, the detection models may be unable to recognize new morphing forms, leaving them open to new kinds of assaults.

Privacy Issues: Sensitive personal data may be needed for effective detection techniques, which may give rise to privacy issues. Face morphing detection systems can be difficult to build and execute because of the requirement to strike a balance between protecting people's privacy and precise detection.[21]

4. Future Scope

This Methodology will be the new evaluation platform for the testing of algorithms and detailed analysis of subsets of sequestered data, In Research on anti-forensic image manipulations to hinder detection and integration of morphing detection in document application and verification stages, Proposed solution shows potential for generalized performance. Combine multiclass pretraining with defense against adversarial attacks, further robustify neural network models against attacks, and obtain better training performance and more reliable results.

5. Conclusion

Detection performance: MAD's, deep face representation-based detection performance is encouraging and remarkably resilient in terms of image post-processing, which includes print-scan modification, resizing, and compression of images. This is an obvious benefit over texture-descriptor- based MAD, which is usually quite sensitive to post-processing, especially in more difficult situations. Furthermore, there is no discernible relationship between the detection performance and the training set that underwent post-processing, such that to train, scanned photos are required. Heterogeneous morphing algorithms: morphs produced by morphing algorithms that result in observable artifacts, such as ghost artifacts that are readily noticeable, are often identified with more precision. Additionally, there is a modest decline in recognition performance if training and evaluation sets comprise morphs produced by various morphing techniques. Machine learning-based classifiers: AdaBoost, Gradient Boosting, Random Forest, and Support Vector are some of the tested models for machine learning. (SVM) and SVM-based classifiers in general had the best effective detection efficiency among the great majority of trials that were carried out. The enhancement of the images' quality and appearance that results from the de-morphing procedure is among the most important factors. Furthermore, the ABC systems process well fits the de- morphing network. Furthermore, the concealed identity of the forger is discovered. There may be a lot of uses for this functionality in the future.

.

REFERENCES

1. Kessler, R., Raja, K., Tapia, J., & Busch, C. (2023). Towards minimizing efforts for Morphing Attacks--Deep embeddings for morphing pair selection and improved Morphing Attack Detection. arXiv preprint arXiv:2305.18216.
2. Fu, B., Spiller, N., Chen, C., & Damer, N. (2021, September). The effect of face morphing on face image quality. In 2021 international conference of the biometrics special interest group (BIOSIG) (pp. 1 -5). IEEE.
3. Seibold, C., Samek, W., Hilsmann, A., & Eisert, P. (2020). Accurate and robust neural networks for face morphing attack detection. Journal of Information Security and applications, 53, 102526.
4. Seibold, C., Samek, W., Hilsmann, A., & Eisert, P. (2017). Detection of face morphing attacks by deep learning. In Digital Forensics and Watermarking: 16th International Workshop, IWDW 2017, Magdeburg, Germany, August23- 25, 2017, Proceedings 16 (pp. 107-120). Springer International Publishing.
5. Merkle, J., Rathgeb, C., Scherhag, U., Busch, C., & Breithaupt, R. (2019). Face morphing detection: issues and challenges. In Proceedings of the international conference on biometrics for borders (ICBB).
6. Korshunov, P., & Marcel, S. (2019). Vulnerability of face recognition to deep morphing. arXiv preprint arXiv:1910.01933.
7. Ortega-Delcampo, D., Conde, C., Palacios-Alonso, D., & Cabello, E. (2020). Border control morphing attack detection with a convolutional neural network de-morphing approach. IEEE Access, 8, 92301-92313.
8. Medvedev, I., Shadmand, F., & Gonçalves, N. (2022). MorDeephy: Face morphing detection via fused classification. arXiv preprint arXiv:2208.03110.
9. Razaq, I. S. (2023). Improved Face Morphing Attack Detection Method Using PCA and Convolutional Neural Network. Karbala International Journal of Modern Science, 9(2), 15.
10. Ivanovska, M., Kronovšek, A., Peer, P., Štruc, V., & Batagelj, B. (2022). Face morphing attack detection using privacy-aware training data. arXiv preprint arXiv:2207.00899.
11. Qin, L., Peng, F., & Long, M. (2022). Face morphing attack detection and localization based on feature-wise supervision. IEEE Transactions on Information Forensics and Security, 17, 3649-3662
12. Venkatesh, S., Ramachandra, R., Raja, K., & Busch, C. (2021). Face morphing attack generation and detection: A comprehensive survey. IEEE transactions on technology and society, 2(3), 128-145.)
13. Venkatesh, S., Ramachandra, R., Raja, K., & Busch, C. (2020, July). Single image face morphing attack detection using ensemble of features. In 2020 IEEE 23rd International Conference on Information Fusion (FUSION) (pp. 1-6). IEEE.
14. Makrushin, A., & Wolf, A. (2018, September). An overview of recent advances in assessing and mitigating the face morphing attack. In 2018 26th European Signal Processing Conference (EUSIPCO) (pp. 1017-1021). IEEE
15. Damer, N., Spiller, N., Fang, M., Boutros, F., Kirchbuchner, F., & Kuijper, A. (2021). Pw-mad: Pixel- wise supervision for generalized face morphing attack detection. In Advances in Visual Computing: 16th International Symposium, ISVC 2021, Virtual Event, October 4 -6, 2021, Proceedings, Part I (pp. 291-304). Springer International Publishing.
16. Ortega-Delcampo, D., Conde, C., Palacios-Alonso, D., & Cabello, E. (2020). Border control morphing attack detection with a convolutional neural network de- morphing approach. IEEE Access, 8, 92301-92313.
17. Scherhag, U., Debiasi, L., Rathgeb, C., Busch, C., & Uhl, A. (2019). Detection of face morphing attacks based on PRNU analysis. IEEE Transactions on Biometrics, Behavior, and Identity Science, 1(4), 302-317.
18. Borghi, G., Pancisi, E., Ferrara, M., & Maltoni, D. (2021). A double siamese framework for differential morphing attack detection. Sensors, 21(10), 3466.
19. Hamza, M., Tehsin, S., Karamti, H., & Alghamdi, N. S. (2022). Generation and detection of face morphing attacks. IEEE Access, 10, 72557-72576.
20. Makrushin, A., & Wolf, A. (2018, September). An overview of recent advances in assessing and mitigating the face morphing attack. In 2018 26th European Signal Processing Conference (EUSIPCO) (pp. 1017- 1021). IEEE
21. Damer, N., López, C. A. F., Fang, M., Spiller, N., Pham, M. V., & Boutros, F. (2022). Privacy-friendly synthetic data for the development of face morphing attack detectors. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (pp. 1606- 1617).