International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Special Issue: 1 Volume No.9 March - April – 2025
DOI:10.46647/ijetms.2025.v09si01.006 ISSN: 2581-4621

Role of Accomplices in Morphing Attacks: A Comprehensive Survey

Naheed Sultana[1]*, T C Swetha Priya [2]

[1] *Assistant Professor, Department of Information Technology, Stanley College of Engineering and Technology for Women, India*

[2] *Assistant Professor, Department of Information Technology, Stanley College of Engineering and Technology for Women, India*

Abstract

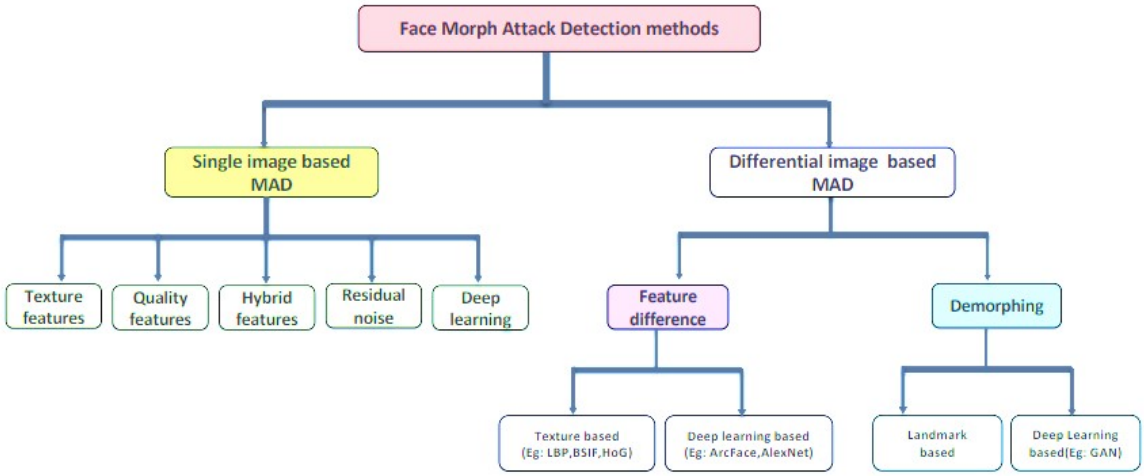
Morphing attacks, where digital objects like images, videos, or biometric information are manipulated to look legitimate while hiding malicious intent, are serious threats to security systems. This extensive survey explores the vital role accomplices play in carrying out morphing attacks. Accomplices can be from human insiders and outside collaborators to automated systems, all of whom play their role in different stages of the attack—ranging from data gathering and morphing methods to delivery and evasion of detection. Human accomplices can help by providing access to sensitive information, controlling security mechanisms, or facilitating social engineering tactics. Simultaneously, botnets and image manipulation tools are potential automated accomplices that can aid in generating and propagating manipulated data. This survey delves into how accomplices cooperate, how this affects the efficacy of morphing attacks, and the cybersecurity implications. Through examining the accomplices' role, this research hopes to better understand morphing attack methods and influence the creation of more effective defense mechanisms.

Keywords: Face recognition, biometrics, morphing attacks, morphing attack detection (MAD), differential MAD (D-MAD)

1. INTRODUCTION

Biometrics is a technique for recognizing individuals based on their unique characteristics. An extensively utilized biometric method is facial recognition. Face morphing is used in fraudulent activities using facial recognition systems [1]. In a The use of digital images for morphing attacks and the use of re-digitized images for morphing attacks are the two main categories of morphing attacks. Preventing morphing attacks requires an understanding of the process and its end traces. However, it is challenging for human viewers to recognize altered facial pictures; so, it is problematic to rely solely on human judgment for detection. It is currently difficult to recognize altered face images because of the development of morphing techniques and the availability of freely accessible software that make it tough to accurately detect morphing attacks. Distinguishing morphing effects from actual facial features many techniques have been proposed to detect morphing attacks, including Morphing Attack Detection (MAD) systems, which are divided into two categories: Differential MAD and Single-image MAD.S-MAD uses deep learning, texture analysis, or frequency analysis to examine a single facial image and identify defects linked to morphing. D-MAD, on the other hand, compares a suspected morphed image with a trusted reference image to identify inconsistencies. While D-MAD has shown promising results, it faces a major limitation: it is effective when the morphed image represents both contributing identities equally but struggles when the morph is biased toward one individual. This reduces biometric

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Special Issue: 1 Volume No.9 March - April – 2025
DOI:10.46647/ijetms.2025.v09si01.006 ISSN: 2581-4621



discrepancies, making detection more challenging.

Fig. 1: Methods Classification for Morphing Attacks

To overcome this limitation, introduces ACIdA, a novel modular D-MAD system that improves detection accuracy. Unlike traditional D-MAD approaches that primarily rely on identity verification, ACIdA integrates multiple components focusing on both identity-based comparison and artifact detection. The system includes (1) a classification module that categorizes identity verification attempts, (2) an identity-artifact analysis module that detects morphing artifacts while performing biometric verification, and (3) a pure identity analysis module that relies on biometric embeddings to differentiate between genuine and morphed images.

Through extensive cross-dataset experimental evaluations, ACIdA demonstrates state-of-the-art performance in detecting both types of morphing attacks. The proposed system significantly enhances the robustness of D-MAD methods by addressing a critical gap in detecting morphing manipulations that are biased toward one contributing individual. This research contributes to improving the security and reliability of biometric authentication systems, ensuring more effective detection of morphing-based identity fraud.

2. FACE MORPH ATTACK GENERATION

To construct morphs, a range of techniques can be employed, from simple image warping to more advanced Generative Adversarial Networks (GAN). The landmark-based methodology, which is the most popular morph generation method, combines the images according to related landmarks. This is done by following a series of structured steps to ensure the blend appears natural and realistic. Initially, facial landmark detection is used to identify important facial features in both donor photos, including the mouth, nose, and eyes [2][7].These landmarks are then blended together using a fixed ratio, typically 0.5, to create an intermediate set of landmarks that represents an average of both faces. Next, the face is divided into small triangular sections, a process known as triangulation, which helps in smoothly aligning the two images. Both donor images are then warped to fit these intermediate landmarks, ensuring that facial features match up correctly. Once aligned, the images are merged through cross-dissolving, blending pixel values to form a seamless transition. This merging can be applied to either the entire face or just the convex hull of the landmark set (the main facial area) to minimize noticeable distortions. Finally, post-processing adjustments are made to remove visual artifacts, such as blurriness or unnatural edges, ensuring that the morphed image appears realistic. Attacks that use face morphing involve taking a large number of faces and combining or averaging them to produce a composite image that resembles a real person. Many fraudulent schemes employ this composite image to imitate actual persons.

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Special Issue: 1 Volume No.9 March - April – 2025
DOI:10.46647/ijetms.2025.v09si01.006 ISSN: 2581-4621

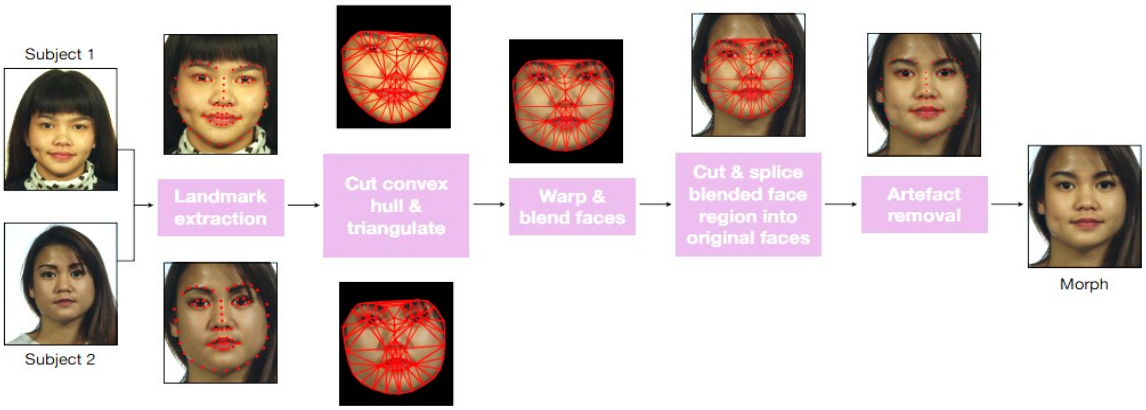


Fig. 2: ***Landmark-Based Morphing Process***

3. FACE MORPHING ATTACK IDENTIFICATION FRAMEWORK

Preparing data, obtaining features, feature preparation, and classifier training are the four primary phases that make up the Morphing Attack Detection system.

Preparing the Data and Extracting Features

Before extracting features, face images must be pre-processed to ensure uniform resolution, alignment, and pose correction by applying the dlib algorithm. This normalization is essential, especially for texture-based methods, to focus on facial details while eliminating background interference [3].

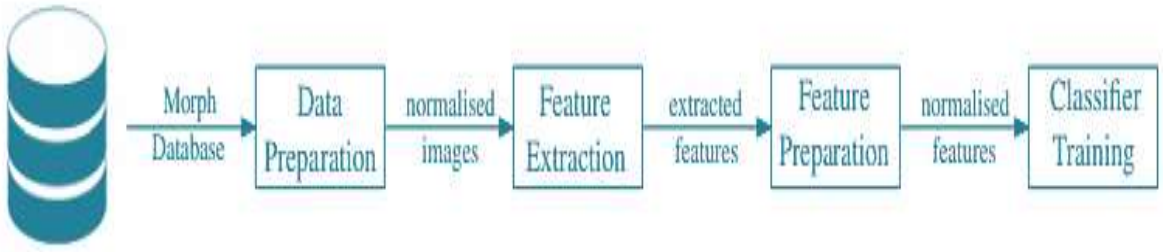


Fig. 3: Face Morphing Detection Framework

Feature Preparation and Classifier Training

Feature vector captures important facial details from an image—such as texture, shape, and patterns—and converts them into numerical values. These numbers act as a unique representation of the image, helping the system analyze and compare faces. A classifier that can distinguish between actual and altered faces is then trained using the feature vectors. To ensure accurate results, most classifiers require the data to be normalized, meaning it is adjusted to a consistent scale for better processing and performance.

4. DATASET PREPARATION FOR MORPHING ANALYSIS

Tests to identify morphing attacks require a large collection of images of transformed faces. These images are efficiently produced using automated morphing algorithms. The dataset is then divided into two halves, one for testing and another for training the model, with care taken to ensure that no participants are included in both sets. S-MAD is primarily tested on PMDB, Idiap Morph, and MorphDB[4], which provide large collections of morphed images without requiring a reference image.D-MAD benefits from FEI Morph, as it allows comparison with a trusted live capture (TLC)

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Special Issue: 1 Volume No.9 March - April – 2025
DOI:10.46647/ijetms.2025.v09si01.006 ISSN: 2581-4621

to detect subtle differences between real and morphed face.

Table 1: Summary of Morphing Image Datasets

Database Name	Total Images	Source Datasets	Subjects	Morphing Algorithms	Key Features
Progressive Morphing Database (PMDB)	1,108	AR, FRGC, Color Feret	280 individuals (134 males, 146 females)	Not specified	No manual retouching; artifacts like blurring and ghost effects; artifact-free background replacement
Idiap Morph	Multiple sets	Feret, FRGC, Face Research Lab London Set	Not specified	OpenCV, FaceMorpher, StyleGAN	OpenCV & FaceMorpher: More artifacts; StyleGAN: Fewer artifacts but retains GAN-related texture patterns
MorphDB	100	Color Feret, FRGC	Not specified	Not specified	Manually retouched for improved visual quality
FEI Morph	6,000	FEI Face Database (200 subjects, equal male-female ratio)	200 subjects (equal male-female ratio)	Not specified	Morphing Variants: 0.3 and 0.5; aimed to detect morphing even in current time is very similar to morphed accomplice

5. MORPH ATTACK DETECTION MODEL

A number of detection methods have been created to improve face recognition systems' resistance to facial changes and stop image counterfeiting. The integrity and authenticity of facial photographs can be confirmed by integrating these algorithms into already-existing face recognition frameworks. Detection techniques aid in ensuring that modified facial photographs are not used for authentication or saved during enrollment in such systems. Two different detection methods are used to detect changed facial photos.

(A). Single-Image Detectors

Single image detection for morphing attacks focuses on identifying alterations or synthetic manipulations within a single biometric image, such as a facial scan or passport photo, without requiring multiple images for comparison [2]. This is accomplished by using texture and feature analysis techniques that identify irregularities in image texture and edges, such as Local Binary Patterns (LBP) and Histogram of Oriented Gradients (HOG). Furthermore, deep learning models such as XceptionNet are extensively utilized, since their capacity to recognize intricate patterns and

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Special Issue: 1 Volume No.9 March - April – 2025
DOI:10.46647/ijetms.2025.v09si01.006 ISSN: 2581-4621

hierarchical elements makes them proficient in identifying picture manipulation. Their ability to adjust to novel attacks such as GAN-based morphing, deepfake-assisted morphing, and adaptive morphing approaches may outperform S-MAD systems that rely on manually constructed features.

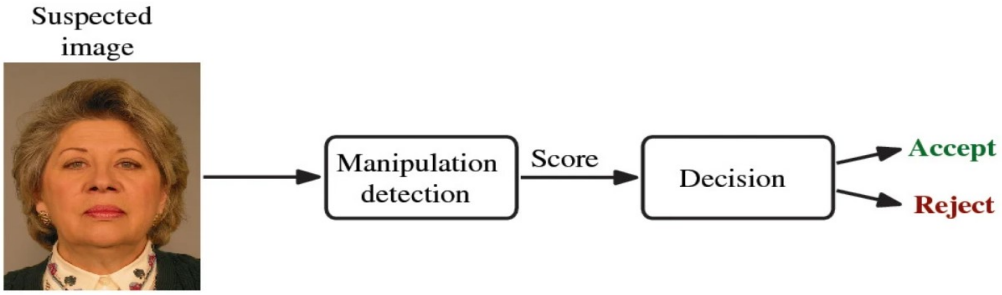


Fig4: No Reference Morphing Detection Scheme

XceptionNet Model

XceptionNet is a deep learning model designed to efficiently process images by breaking down the filtering process into two steps: one for detecting patterns and another for handling colors. This makes it faster and more accurate, especially for tasks like deepfake detection [5].The model also includes residual connections, which help it learn better and avoid losing important details during training. Its structure consists of multiple layers of special convolutions, pooling, and connections that improve performance. Because of its ability to detect fine details and subtle changes, XceptionNet is widely used for identifying fake images and deepfake videos, making it a strong tool for forgery detection systems.

Training Phase:

In groups of 32–64, XceptionNet analyzes 299×299×3 photos to detect morphing assaults. Residual connections and depthwise separable convolutions are used to capture complex patterns. For binary or multi-class data, the output layer uses Sigmoid logic or Softmax, while the hidden layer grouping uses ReLU. Cross-entropy and the Adam optimizer are used to train the model in either a binary or categorical manner. It frequently strikes a balance between efficiency and accuracy during 30 to 50 epochs.

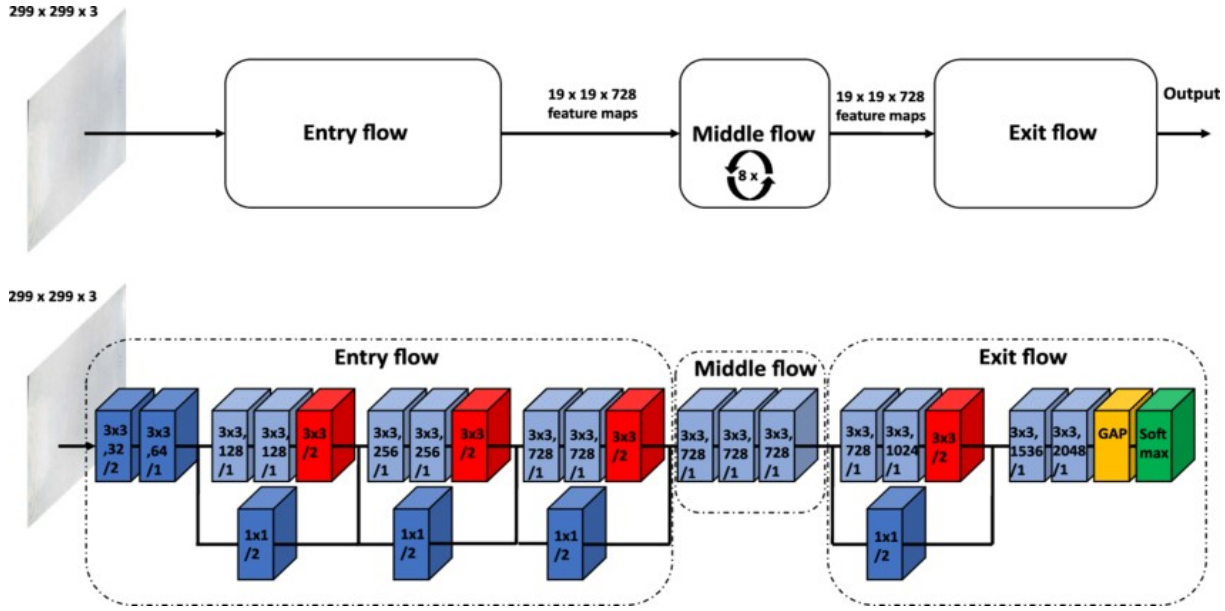


Fig5: Detailed design of the original Xception model, including spatial convolution blocks and batch normalization

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Special Issue: 1 Volume No.9 March - April – 2025
DOI:10.46647/ijetms.2025.v09si01.006 ISSN: 2581-4621

Testing Phase:

In testing, XceptionNet classifies new images as real or morphed or detects multiple morphing techniques. It uses Sigmoid for binary and Softmax for multi-class outputs. Its efficient architecture accurately detects subtle morphing artifacts, ensuring high accuracy with low computational cost.

(B). Differential Detector

Differential Morphing Attack Detection (MAD) is a method for determining if a face image has undergone morphing manipulation. There are two primary methods for detecting this. The first method compares features taken from two images directly: a real probing image and a reference image that may have been altered [2]. After comparing these feature vectors, machine learning models determine if the comparison is a morphing attack (MA) or a true (bona fide) match. The second method, called de-morphing, makes use of the probe picture to try to undo the morphing process. Ideally, de-morphing should recreate the second face if the reference image was made by blending two distinct faces, indicating that the image was transformed. This recreated face can then be compared to the probing image by a biometric face recognition system to ascertain validity. Using pre-trained deep networks can increase detection accuracy, but creating a deep learning model from scratch necessitates a large amount of data.

It relies on differential features by comparing a live image with a trusted reference image. Techniques like ArcFace and FaceNet are used to extract high-dimensional identity embeddings from both images[6]. These embeddings are then compared using cosine similarity to measure the degree of similarity between the two images. If the similarity score is below a predefined threshold, the pair is flagged as potentially morphed. This approach is highly effective because it captures identity-specific discrepancies that are difficult to manipulate consistently in morphs. Unlike S-MAD, which uses a binary classifier, D-MAD relies on similarity score-based comparisons to detect inconsistencies between the live and reference images[8].

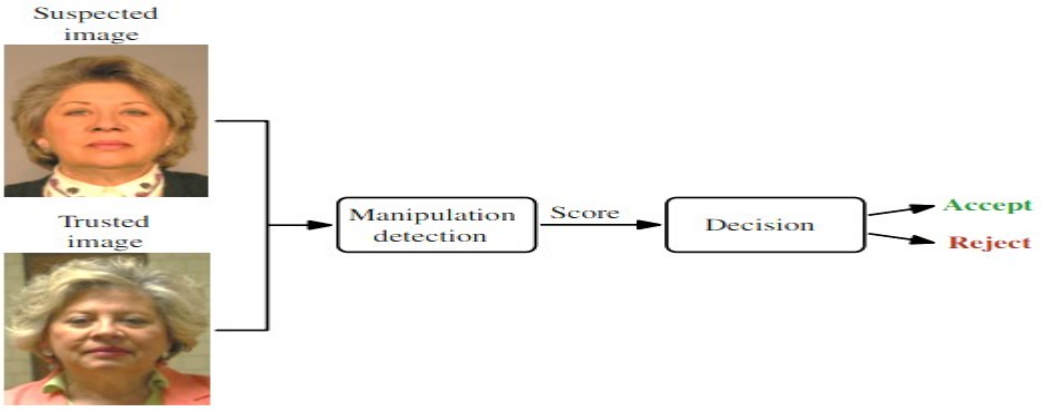


Fig6: Differential Morphing Detection Scheme

Deep Embedding : Cosine Similarity

Plays a significant role in identifying morphing attacks. It first looks at how different Facial Recognition Systems (FRSs) create face embeddings to automatically choose images for making morphed faces. By measuring the distance between these embeddings, shows an easy way to create a large set of morphed images. It then tests how well this method works by checking how easily deep learning-based FRSs and two commercial FRSs are fooled by the morphed images. Helps in understanding and improving the security of FRSs against morphing attacks [6].

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Special Issue: 1 Volume No.9 March - April – 2025
DOI:10.46647/ijetms.2025.v09si01.006 ISSN: 2581-4621

Four distinct architectures were chosen in order to acquire the embeddings for our pre-selection pipeline. VGG-Face, DeepFace, MagFace, and ArcFace were our selections. To calculate the degree of similarity between embeddings, which usually contain substantial identity-preserving data. Given two embedding vectors of equal size, we computed the similarity between the underlying faces using the cosine distance [6].

Fig 7: Embeddings per FRS.

To find the cosine distance between two embedding's that represent two face photos, use the formula: E1 and E2 are the D-dimensional embedding vectors of the picture.

$$d_{cos}(E_1, E_2) = 1 - \frac{E_1^T E_2}{||E_1|| \cdot ||E_2||}$$

Four morphing algorithms were employed: one deep learning-based technique, MIPGAN, which integrated the latent space of two images, and three landmark-based methods, Alyssaq Morpher, NTNU Morpher, and UBO Morpher, which averaged 68 facial landmarks extracted using OpenCV dlib. All used a morphing factor of 0.5.

6. PERFORMANCE METRICS

This section discusses MAD systems' performance measures

1. Error Rate for Attack Presentation Classification (APCER): Indicates how frequently modified photos are mistakenly identified as authentic. It shows how susceptible the system is to morphing attacks [2].

APCER= FP/FP+TN
FP = False Positives (Morphed images classified as genuine)
TN = True Negatives (Genuine images correctly classified)

2. **Error Rate for Bonafide Presentation Classification (BPCER):** Determines how frequently real photos are mistakenly labeled as altered. It displays the system's rate of false rejections.

BPCER= FN/FP+TN
FN = False Negatives (Genuine images classified as morphed)
TP = True Positives (Morphed images correctly classified)

3. **Equal Error Rate for Detection(D-EER):** Equilibrium between false positives and false

FRS	# of embeddings
ArcFace	512
DeepFace	4096
VGG-Face	2622
MagFace	512

negatives, which is reached when APCER and BPCER are equal. A reduced D-EER is a sign of improved performance.

APCER = BPCER.

4. Rate of True Positive: Determines the percentage of modified photos that are successfully identified. It demonstrates how well the technology can detect.

DOI:10.46647/ijetms.2025.v09si01.006 ISSN: 2581-4621

TPR= TP/ TP+FN

5. Area Under the Receiver Operating Characteristic Curve (AUC): Symbolizes the model's capacity to discriminate between real and altered images. A higher AUC indicates better performance.

.

ACC= Accurate Classification/Total Classified Image

7. CONCLUSIONS

An extensive review of morphing generation methods, detection frameworks, pertinent datasets, and assessment techniques is given in this survey. It examines different morphing generation techniques, emphasizing how intricate and successful they are at getting around biometric systems. With the use of sophisticated algorithms and identity verification methods, the detection frameworks under study show methodical approaches to morphing artifact detection. Diverse datasets were analyzed, emphasizing the importance of cross-dataset validation for reliable performance. Evaluation metrics such as APCER, BPCER, and D-EER were discussed to assess detection accuracy and robustness. Continued advancement in detection methods and standardized evaluation metrics is crucial for enhancing the security of biometric authentication systems against sophisticated morphing attacks.

REFERENCES

1. Rawat, G., Gupta, H., Faisal, S., & Hashir, M. (2024). Face Morphing Attack Detection-A Literature Review. International Journal of Biomedical Research and Health Sciences, 2(1)
2. Autherith, S., & Pasquini, C. (2025). Detecting Morphing Attacks through Face Geometry Features. Department of Computer Science, University of Innsbruck, Austria; Department of Information Engineering and Computer Science, University of Trento, Italy.
3. Scherhag, U., Rathgeb, C., & Busch, C. (2022). Face Morphing Attack Detection Methods. In Handbook of Digital Face Manipulation and Detection (pp. [specific pages]). Springer. DOI link
4. Di Domenico, N., Borghi, G., Franco, A., & Maltoni, D. (2025). Improving Accomplice Detection in the Morphing Attack. Machine Intelligence Research, 1-14. https://doi.org/10.1007/s11633-024-1533-1
5. B. Yasser, J. Hani, S. El-gayar, O. Amgad, N. Ahmed, H. M. Ebied, H. Amr, and M. Salah, "Deepfake Detection Using EfficientNet and XceptionNet," 2022 International Conference on Innovative Trends in Computer Engineering (ITCE), Aswan, Egypt, 2022, pp. 1-6.
6. Di Domenico, N., Borghi, G., Franco, A., & Maltoni, D. (2024). *Dealing with Subject Similarity in Differential Morphing Attack Detection*. arXiv:2404.07667.
7. 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. https://doi.org/10.1109/TTS.2021.3066254
8. M. Ibsen, C. Rathgeb, D. Fischer, P. Drozdowski, and C. Busch, "Digital face manipulation in biometric systems," in Handbook of Digital Face Manipulation and Detection: From DeepFakes to Morphing Attacks, R. Tolosana, R. Vera-Rodriguez, J. Fierrez, A. Morales, and J. Ortega-Garcia, Eds. Springer, 2022, pp. 27–43. doi: 10.1007/978-3-030-87664-7_2.
9. Raja, K., Gupta, G., Venkatesh, S., Ramachandra, R., & Busch, C. (Year). Towards Generalized Morphing Attack Detection by Learning Residuals. Norwegian University of Science and Technology, Norway.